SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 154° - Numero 172

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA **Roma - Mercoledì, 24 luglio 2013** SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DIREZIONE E REDAZIONE PRESSO IL MINISTERO DELLA GIUSTIZIA - UFFICIO PUBBLICAZIONE LEGGI E DECRETI - VIA ARENULA, 70 - 00186 ROMA
AMMINISTRAZIONE PRESSO L'ISTITUTO POLIGRAFICO E ZECCA DELLO STATO - VIA SALARIA, 1027 - 00138 ROMA - CENTRALINO 06-85081 - LIBRERIA DELLO STATO PIAZZA G. VERDI, 1 - 00198 ROMA

La **Gazzetta Ufficiale, Parte Prima,** *oltre alla* **Serie Generale**, *pubblica cinque Serie speciali, ciascuna contraddistinta da autonoma numerazione:*
- **1ª Serie speciale:** *Corte costituzionale (pubblicata il mercoledì)*
- **2ª Serie speciale:** *Comunità europee (pubblicata il lunedì e il giovedì)*
- **3ª Serie speciale:** *Regioni (pubblicata il sabato)*
- **4ª Serie speciale:** *Concorsi ed esami (pubblicata il martedì e il venerdì)*
- **5ª Serie speciale:** *Contratti pubblici (pubblicata il lunedì, il mercoledì e il venerdì)*

La **Gazzetta Ufficiale, Parte Seconda,** "Foglio delle inserzioni", *è pubblicata il martedì, il giovedì e il sabato*

AVVISO ALLE AMMINISTRAZIONI

Al fine di ottimizzare la procedura di pubblicazione degli atti in *Gazzetta Ufficiale,* le Amministrazioni sono pregate di inviare, contemporaneamente e parallelamente alla trasmissione su carta, come da norma, anche copia telematica dei medesimi (in formato word) al seguente indirizzo di posta elettronica certificata: gazzettaufficiale@giustiziacert.it, curando che, nella nota cartacea di trasmissione, siano chiaramente riportati gli estremi dell'invio telematico (mittente, oggetto e data).

Nel caso non si disponga ancora di PEC, e fino all'adozione della stessa, sarà possibile trasmettere gli atti a: gazzettaufficiale@giustizia.it

SOMMARIO

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Nebivololo Ranbaxy» *(13A06212)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Neisvac-C» *(13A06213)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Fluarix» *(13A06214)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Montelukast Aurobindo» *(13A06215)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Atorvastatina Krka». *(13A06216)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Montelukast Pfizer Italia». *(13A06217)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Metocal Vitamina D3». *(13A06218)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Diflucan» *(13A06219)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Valaciclovir Sandoz». *(13A06220)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Vinblastina Teva» *(13A06221)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Amisulpride EG» *(13A06222)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Genotropin» *(13A06223)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Roferon A» *(13A06224)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Omeprazolo Sandoz Bv» *(13A06225)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Rizatriptan Zentiva Italia» *(13A06226)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Alfuzosina Pfizer» *(13A06227)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «BCG Medac» *(13A06228)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Gliclazide Eurogenerici». *(13A06229)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Aggrastat» *(13A06230)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Famciclovir Actavis». *(13A06231)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Desogestrel Mylan». *(13A06232)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Humulin» *(13A06233)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Aranda» *(13A06234)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Levofloxacina EG». *(13A06235)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Ondansetron Crinos» *(13A06236)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Onnua» *(13A06237)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Riastap» *(13A06238)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Claritromicina Teva» *(13A06239)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Augmentin» *(13A06240)*

Modificazione dell'autorizzazione all'immissione in commercio del medicinale per uso umano «Candesartan e Idroclorotiazide Hexal». *(13A06241)*

Modificazione dell’autorizzazione all’immissione in commercio del medicinale per uso umano «Azalia» *(13A06242)*

Modificazione dell’autorizzazione all’immissione in commercio del medicinale per uso umano «Bicalutamide Teva». *(13A06243)*

Modificazione dell’autorizzazione all’immissione in commercio del medicinale per uso umano «Nicotinell Mint». *(13A06244)*

Modificazione dell’autorizzazione all’immissione in commercio del medicinale per uso umano «Octreotide Hospira». *(13A06245)*

Modificazione dell’autorizzazione all’immissione in commercio del medicinale per uso umano «Elidel». *(13A06246)*

Modificazione dell’autorizzazione all’immissione in commercio del medicinale per uso umano «Octreoscan». *(13A06247)*

Modificazione dell’autorizzazione all’immissione in commercio del medicinale per uso umano «Alendronato Teva». *(13A06248)*

Modificazione dell’autorizzazione all’immissione in commercio del medicinale per uso umano «Sevoflurane Baxter». *(13A06249)*

Modificazione dell’autorizzazione all’immissione in commercio del medicinale per uso umano «Taxceus». *(13A06250)*

Modificazione dell’autorizzazione all’immissione in commercio del medicinale per uso umano «Clopidogrel Doc Generici». *(13A06251)*

Modificazione dell’autorizzazione all’immissione in commercio del medicinale per uso umano «Nacrez» *(13A06252)*

Modificazione dell’autorizzazione all’immissione in commercio del medicinale per uso umano «Pantoprazolo Sun». *(13A06253)*

Rinnovo dell’autorizzazione all’immissione in commercio, secondo procedura di mutuo riconoscimento, del medicinale per uso umano «Fevralt», con conseguente modifica stampati. *(13A06254)*

Rinnovo dell’autorizzazione all’immissione in commercio, secondo procedura di mutuo riconoscimento, del medicinale per uso umano «Metformina Doc Generici», con conseguente modifica stampati. *(13A06255)*

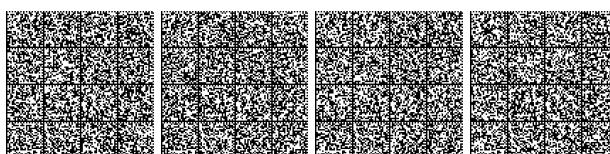
Rinnovo dell’autorizzazione all’immissione in commercio, secondo procedura nazionale, del medicinale per uso umano ATENOLOLO E CLORTALIDONE MYLAN GENERICS, con conseguente modifica stampati. *(13A06256)*

Rinnovo dell’autorizzazione all’immissione in commercio, secondo procedura nazionale, del medicinale per uso umano ATENOLOLO ALTER, con conseguente modifica stampati. *(13A06257)*

Rinnovo dell’autorizzazione all’immissione in commercio, secondo procedura di mutuo riconoscimento, del medicinale per uso umano CONFIDEX, con conseguente modifica stampati. *(13A06258)*

Rinnovo dell’autorizzazione all’immissione in commercio, secondo procedura di mutuo riconoscimento, del medicinale per uso umano OLANZAPINA EG, con conseguente modifica stampati. *(13A06259)*

Proroga smaltimento scorte del medicinale per uso umano «Valsacombi» *(13A06260)*

Proroga smaltimento scorte del medicinale per uso umano «Glamin» *(13A06261)*

DECRETI, DELIBERE E ORDINANZE MINISTERIALI

MINISTERO DELLA SALUTE

DECRETO 1° marzo 2013.

Autorizzazione all'immissione in commercio del prodotto fitosanitario «Troy 480».

IL DIRETTORE GENERALE
PER L'IGIENE E LA SICUREZZA DEGLI ALIMENTI
E DELLA NUTRIZIONE

Visto l'art. 6 della legge 30 aprile 1962, n. 283, modificato dall'art. 4 della legge 26 febbraio 1963, n. 441;

Visto il decreto legislativo 30 marzo 2001, n. 165, che detta norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche;

Vista la legge 13 novembre 2009, n. 172 concernente «Istituzione del Ministero della salute e incremento del numero complessivo dei sottosegretari di Stato»;

Visto il decreto del Presidente della Repubblica 11 marzo 2011, n. 108, recante il Regolamento di riorganizzazione del Ministero della salute;

Visto il decreto del Ministro della salute 2 agosto 2011 concernente la disciplina transitoria dell'assetto organizzativo del Ministero della salute;

Visto il decreto legislativo 17 marzo 1995, n. 194, concernente l'attuazione della direttiva 91/414/CEE in materia d'immissione in commercio di prodotti fitosanitari, nonché la circolare del 10 giugno 1995, n. 17 (Supplemento ordinario alla *Gazzetta Ufficiale* n. 145 del 23 giugno 1995) concernenti «Aspetti applicativi delle nuove norme in materia di autorizzazione di prodotti fitosanitari»;

Visto il decreto del Presidente della Repubblica 23 aprile 2001, n. 290 concernente il regolamento di semplificazione dei procedimenti di autorizzazione alla produzione, all'immissione in commercio e alla vendita di prodotti fitosanitari e relativi coadiuvanti, come modificato dal decreto del Presidente della Repubblica 28 febbraio 2012, n. 55, concernente il regolamento di modifica del decreto del Presidente della Repubblica 23 aprile 2001, n. 290;

Visto il Regolamento (CE) n. 1107/2009 del Parlamento europeo e del Consiglio del 21 ottobre 2009 relativo all'immissione sul mercato dei prodotti fitosanitari e che abroga le direttive del Consiglio 79/117/CEE e 91/414/CEE ed in particolare l'art. 80 concernente «misure transitorie»;

Visti i Regolamenti (UE) della Commissione n. 540/2011, n. 541/2011, n. 544/2011, n. 545/2011, n. 546/2011, n. 547/2011, di attuazione del Regolamento (CE) n. 1107/2009;

Visti il decreto legislativo 14 marzo 2003, n. 65, corretto ed integrato dal decreto legislativo 28 luglio 2004, n. 260, e il decreto ministeriale 3 aprile 2007, concernenti l'attuazione delle direttive 1999/45/CE, 2001/60/CE e 2006/8/CE, relative alla classificazione, all'imballaggio e all'etichettatura dei preparati pericolosi;

Visto il Regolamento (CE) n. 1272/2008 del Parlamento europeo e del Consiglio del 16 dicembre 2008 e il successivo regolamento n. 790/2009 della Commissione del 10 agosto 2009 di adeguamento al progresso tecnico e scientifico, relativi alla classificazione, all'etichettatura e all'imballaggio delle sostanze e delle miscele;

Visto il Regolamento (CE) n. 396/2005 del Parlamento europeo e del Consiglio del 23 febbraio 2005 e successivi aggiornamenti concernenti i livelli massimi di residui di antiparassitari nei o sui prodotti alimentari e mangimi di origine vegetale e animale e che modifica la direttiva 91/414/CEE del Consiglio;

Visto il decreto del Ministero della salute 28 settembre 2012 di rideterminazione delle tariffe relative all'immissione in commercio dei prodotti fitosanitari a copertura delle prestazioni sostenute e rese a richiesta, in attuazione del Regolamento (CE) 1107/2009;

Vista la domanda del 23 novembre 2005 presentata dall'impresa Agrichem BV, con sede legale in Industrieterrein Weststad, Koopvaardijweg 9, Postbus 295, 4900ag, Oosterhout (Olanda), diretta ad ottenere la registrazione del prodotto fitosanitario denominato Troy 480 contenente la sostanza attiva bentazone;

Visto il decreto del 3 aprile 2001 di inclusione della sostanza attiva bentazone, nell'allegato I del decreto legislativo 17 marzo 1995, n. 194 fino al 31 luglio 2011 in attuazione della direttiva 2000/68/CE della Commissione del 23 ottobre 2000;

Visto il decreto del 30 dicembre 2010 di proroga della scadenza dell'inclusione della sostanza attiva bentazone, nell'allegato I del decreto legislativo 17 marzo 1995, n. 194 fino al 31 dicembre 2015 in attuazione della direttiva 2010/77/UE della Commissione del 10 novembre 2010;

Considerato che la direttiva 91/414/CEE è stata sostituita dal Reg. CE n. 1107/2009 e che pertanto la sostanza attiva in questione ora è considerata approvata ai sensi del suddetto Regolamento e riportata nell'allegato al Regolamento UE n. 540/2011;

Visto il parere favorevole espresso in data 16 gennaio 2013 dalla Commissione consultiva di cui all'art. 20 del decreto legislativo 17 marzo 1995, n. 194 relativo all'autorizzazione fino al 31 dicembre 2015, del prodotto fitosanitario in questione;

Vista la nota dell'ufficio in data 22 gennaio 2013 con la quale sono stati richiesti gli atti definitivi per il proseguimento dell'*iter* di autorizzazione

Vista la nota pervenuta in data 4 febbraio 2013 da cui risulta che l'impresa Agrichem BV ha presentato la documentazione richiesta dall'ufficio;

Ritenuto di autorizzare il prodotto Troy 480 fino al 31 dicembre 2015 data di scadenza dell'approvazione della sostanza attiva bentazone;

Visto il pagamento della tariffa a norma del decreto ministeriale 9 luglio 1999, in vigore alla data di presentazione della domanda;

Decreta:

L'impresa Agrichem BV, con sede legale in Industrieterrein Weststad, Koopvaardijweg 9, Postbus 295, 4900ag, Oosterhout (Olanda), è autorizzata ad immettere in commercio il prodotto fitosanitario denominato Troy 480 con la composizione e alle condizioni indicate nell'etichetta allegata al presente decreto, fino al 31 dicembre 2015, data di scadenza dell'iscrizione della sostanza attiva bentazone riportata nell'allegato al Regolamento UE n. 540/2011.

È fatto salvo ogni eventuale successivo adempimento ed adeguamento delle condizioni di autorizzazione del prodotto fitosanitario, anche in conformità a provvedimenti comunitari e ulteriori disposizioni riguardanti le sostanze attive componenti.

Il prodotto è confezionato nelle taglie da l. 1 - 3 - 5 - 6 - 10.

Il prodotto in questione è importato in confezioni pronte per l'impiego dallo stabilimento dell'impresa estera: AgriChem B.V., Koopvaardijweg 9, 4906 CV Oosterhout (Olanda).

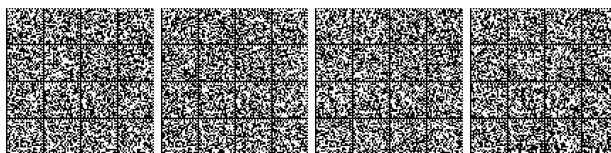
Il prodotto fitosanitario suddetto è registrato al n. 13027.

È approvata quale parte integrante del presente decreto l'etichetta allegata con la quale il prodotto deve essere posto in commercio.

Il presente decreto sarà notificato, in via amministrativa, all'impresa interessata e pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 1° marzo 2013

Il direttore generale: BORRELLO

ALLEGATO

TROY 480

LIQUIDO SOLUBILE

Diserbante di post-emergenza per fagiolo e fagiolino

Composizione:
100 g di prodotto contengono
Bentazone puro g 40.8 (=480 g/L)
Coformulanti q.b. a g 100

IRRITANTE

FRASI DI RISCHIO
Irritante per gli occhi. Può provocare sensibilizzazione per contatto con la pelle. Nocivo per gli organismi acquatici. Può provocare a lungo termine effetti negativi per l'ambiente acquatico.

CONSIGLI DI PRUDENZA
Conservare fuori della portata dei bambini. Conservare lontano da alimenti o mangimi e da bevande. Non mangiare, né bere, né fumare durante l'impiego. Evitare il contatto con gli occhi e con la pelle. Usare indumenti protettivi e guanti adatti e proteggersi gli occhi/la faccia. In caso d'ingestione consultare immediatamente il medico e mostrargli il contenitore o l'etichetta. Non disperdere nell'ambiente. Riferirsi alle istruzioni speciali/schede informative in materia di sicurezza.

AGRICHEM B.V., Koopvaardijweg 9, 4906 CV, Oosterhout – Olanda
Tel. 0031 162 431 931

AgriChem

Autorizzazione Ministero della Salute n. del
Officina di produzione: AgriChem B.V., Koopvaardijweg 9, 4906 CV Oosterhout, Olanda
Distribuito da: CEREXAGRI ITALIA S.r.l., Via Terni, 275 – 47522 S. Carlo di Cesena (FC) – Tel.+39 0547 661523 // Chimiberg (divisione Agricoltura di DIACHEM SpA) - via Tonale, 15 - 24061 Albano S. Alessandro (BG) - Tel. +39 035 581 120
Contenuto netto: litri 1-3-5-6-10 **Partita n.**

PRESCRIZIONI SUPPLEMENTARI
Non contaminare l'acqua con il prodotto o il suo contenitore. Per proteggere le acque sotterranee non applicare su suoli contenenti una percentuale di sabbia superiore all'80%.

INFORMAZIONI PER IL MEDICO
Sintomi: la sostanza è rapidamente assorbita e rapidamente escreta invariata per via urinaria. Irritante perla cute e per le mucose oculari e degli apparati gastrointestinale e respiratorio. Dopo ingestione: nausea, vomito, diarrea, dispnea, tremori, astenia. Negli animali da esperimento: eccitamento del S.N.C.
Terapia: sintomatica.
Consultare un Centro Antiveleni

CARATTERISTICHE TECNICHE
TROY 480 è un erbicida fogliare di contatto; viene assorbito principalmente dalle parti verdi della pianta ed in parte traslocato. TROY 480 si impiega, quindi, solo in post-emergenza della coltura e delle infestanti.
Il prodotto è efficace contro: *Amaranthus retroflexus* (Amaranto comune), *Anagallis arvensis* (Mordigallina), *Chenopodium album* (Farinaccio comune), *Cyperus rotundus* (Zigolo infestante), *Convolvulus arvensis* (Vilucchio), *Galinsoga parviflora* (Galinsoga comune), *Lamium amplexicaule* (Falsa ortica reniforme), *Matricaria* spp. (Camomilla), *Mercurialis annua* (Mercorella comune), *Polygonum persicaria* (Persicaria), *Polygonum lapatifolium* (Poligono nodoso), *Portulaca oleracea* (Erba porcellana), *Sinapis arvensis* (Senape selvatica), *Sonchus arvensis* (Grespino dei campi), *Stellaria media* (Centocchio).

DOSI, EPOCHE E MODALITÀ DI IMPIEGO
Fagiolo e fagiolino 3 litri per ettaro; il trattamento si effettua a partire da un'altezza di 8-10 cm della coltura e con infestanti nelle prime fasi di sviluppo. In tutte le applicazioni il prodotto va impiegato con volumi di acqua di 400-500 L/ha.
AVVERTENZE: Perché una quantità sufficiente di prodotto possa essere assorbita dalle infestanti, è necessario che non si verifichi una pioggia per diverse ore dopo il trattamento (12-24 ore). TROY 480 non è volatile e può essere applicato anche in vicinanza delle colture sensibili agli erbicidi ormonici (vigneti, frutteti, colture orticole).
COMPATIBILITÀ: Il prodotto non è miscibile con insetticidi.
Avvertenza: in caso di miscela con altri formulati deve essere rispettato il periodo di carenza più lungo. Devono inoltre essere osservate le norme precauzionali prescritte per i prodotti più tossici. Qualora si verificassero casi di intossicazione informare il medico della miscelazione compiuta.
FITOTOSSICITÀ: Il prodotto può essere fitotossico per le colture non indicate in etichetta.
SOSPENDERE I TRATTAMENTI 30 GIORNI PRIMA DELLA RACCOLTA PER FAGIOLO E FAGIOLINO.
ATTENZIONE
Da impiegarsi esclusivamente per gli usi e alle condizioni riportate in questa etichetta. Chi impiega il prodotto è responsabile degli eventuali danni derivanti da uso improprio del preparato. Il rispetto di tutte le indicazioni contenute nella presente etichetta è condizione essenziale per assicurare l'efficacia del trattamento e per evitare danni alle piante, alle persone ed agli animali. Non applicare con i mezzi aerei. Per evitare rischi per l'uomo e per l'ambiente seguire le istruzioni per l'uso (art. 9, comma 3, D. L.vo n. 65/2003). Operare in assenza di vento. Da non vendersi sfuso. Smaltire le confezioni secondo le norme vigenti. Il contenitore completamente svuotato non deve essere disperso nell'ambiente. Il contenitore non può essere riutilizzato.

Etichetta autorizzata con decreto dirigenziale del 1 MAR. 2013

13A06325

DECRETO 1° marzo 2013.

Autorizzazione all'immissione in commercio del prodotto fitosanitario «Vivendi 100».

IL DIRETTORE GENERALE
PER L'IGIENE E LA SICUREZZA DEGLI ALIMENTI
E DELLA NUTRIZIONE

Visto l'art. 6 della legge 30 aprile 1962, n. 283, modificato dall'art. 4 della legge 26 febbraio 1963, n. 441;

Visto il decreto legislativo 30 marzo 2001, n. 165, che detta norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche;

Vista la legge 13 novembre 2009, n. 172 concernente «Istituzione del Ministero della salute e incremento del numero complessivo dei sottosegretari di Stato»;

Visto il decreto del Presidente della Repubblica 11 marzo 2011, n. 108, recante il Regolamento di riorganizzazione del Ministero della salute;

Visto il decreto del Ministro della salute 2 agosto 2011 concernente la disciplina transitoria dell'assetto organizzativo del Ministero della salute;

Visto il decreto legislativo 17 marzo 1995, n. 194, concernente l'attuazione della direttiva 91/414/CEE in materia d'immissione in commercio di prodotti fitosanitari, nonché la circolare del 10 giugno 1995, n. 17 (Supplemento ordinario alla *Gazzetta Ufficiale* n. 145 del 23 giugno 1995) concernenti «Aspetti applicativi delle nuove norme in materia di autorizzazione di prodotti fitosanitari»;

Visto il decreto del Presidente della Repubblica 23 aprile 2001, n. 290 concernente il regolamento di semplificazione dei procedimenti di autorizzazione alla produzione, all'immissione in commercio e alla vendita di prodotti fitosanitari e relativi coadiuvanti, come modificato dal decreto del Presidente della Repubblica 28 febbraio 2012, n. 55, concernente il regolamento di modifica del decreto del Presidente della Repubblica 23 aprile 2001, n. 290;

Visto il Regolamento (CE) n. 1107/2009 del Parlamento europeo e del Consiglio del 21 ottobre 2009 relativo all'immissione sul mercato dei prodotti fitosanitari e che abroga le direttive del Consiglio 79/117/CEE e 91/414/CEE ed in particolare l'art. 80 concernente «misure transitorie»;

Visti i Regolamenti (UE) della Commissione n. 540/2011, n. 541/2011, n. 544/2011, n. 545/2011, n. 546/2011, n. 547/2011, di attuazione del Regolamento (CE) n. 1107/2009;

Visti il decreto legislativo 14 marzo 2003, n. 65, corretto ed integrato dal decreto legislativo 28 luglio 2004, n. 260, e il decreto ministeriale 3 aprile 2007, concernenti l'attuazione delle direttive 1999/45/CE, 2001/60/CE e 2006/8/CE, relative alla classificazione, all'imballaggio e all'etichettatura dei preparati pericolosi;

Visto il Regolamento (CE) n. 1272/2008 del Parlamento europeo e del Consiglio del 16 dicembre 2008 e il successivo regolamento n. 790/2009 della Commissione del 10 agosto 2009 di adeguamento al progresso tecnico e scientifico, relativi alla classificazione, all'etichettatura e all'imballaggio delle sostanze e delle miscele;

Visto il Regolamento (CE) n. 396/2005 del Parlamento europeo e del Consiglio del 23 febbraio 2005 e successivi aggiornamenti concernenti i livelli massimi di residui di antiparassitari nei o sui prodotti alimentari e mangimi di origine vegetale e animale e che modifica la direttiva 91/414/CEE del Consiglio;

Visto il decreto del Ministero della salute 28 settembre 2012 di rideterminazione delle tariffe relative all'immissione in commercio dei prodotti fitosanitari a copertura delle prestazioni sostenute e rese a richiesta, in attuazione del Regolamento (CE) 1107/2009;

Vista la domanda del 29 settembre 2004 e successive integrazioni di cui l'ultima del 12 settembre 2011 presentata dall'impresa Agrichem BV, con sede legale in Industrieterrein Weststad, Koopvaardijweg 9, Postbus 295, 4900ag, Oosterhout (Olanda), diretta ad ottenere la registrazione del prodotto fitosanitario denominato Vivendi 100 contenente la sostanza attiva clopiralyd;

Visto il decreto del 20 febbraio 2007 di inclusione della sostanza attiva clopiralyd, nell'allegato I del decreto legislativo 17 marzo 1995, n. 194 fino al 30 aprile 2017 in attuazione della direttiva 2006/64/CE della Commissione del 16 luglio 2006;

Considerato che la direttiva 91/414/CEE è stata sostituita dal Reg. CE n. 1107/2009 e che pertanto la sostanza attiva in questione ora è considerata approvata ai sensi del suddetto Regolamento e riportata nell'allegato al Regolamento UE n. 540/2011;

Visto il parere favorevole espresso in data 16 gennaio 2013 dalla Commissione consultiva di cui all'art. 20 del decreto legislativo 17 marzo 1995, n. 194 relativo all'autorizzazione fino al 31 dicembre 2015, del prodotto fitosanitario in questione;

Vista la nota dell'ufficio in data 22 gennaio 2013 con la quale sono stati richiesti gli atti definitivi per il proseguimento dell'*iter* di autorizzazione;

Vista la nota pervenuta in data 4 febbraio 2013 da cui risulta che l'impresa Agrichem BV ha presentato la documentazione richiesta dall'ufficio;

Ritenuto di autorizzare il prodotto Vivendi 100 fino al 30 aprile 2017 data di scadenza dell'approvazione della sostanza attiva clopiralyd;

Visto il pagamento della tariffa a norma del decreto ministeriale 9 luglio 1999, in vigore alla data di presentazione della domanda;

Decreta:

L'impresa Agrichem BV, con sede legale in Industrieterrein Weststad, Koopvaardijweg 9, Postbus 295, 4900ag, Oosterhout (Olanda), è autorizzata ad immettere in commercio il prodotto fitosanitario denominato Vivendi 100 con la composizione e alle condizioni indicate nell'etichetta allegata al presente decreto, fino al 30 aprile 2017, data di scadenza dell'iscrizione della sostanza attiva clopiralyd riportata nell'allegato al Regolamento UE n. 540/2011.

È fatto salvo ogni eventuale successivo adempimento ed adeguamento delle condizioni di autorizzazione del prodotto fitosanitario, anche in conformità a provvedimenti comunitari e ulteriori disposizioni riguardanti le sostanze attive componenti.

Il prodotto è confezionato nelle taglie da l. 1 - 5 - 10 - 20.

Il prodotto in questione è importato in confezioni pronte per l'impiego dallo stabilimento dell'impresa estera: AgriChem B.V., Koopvaardijweg 9, 4906 CV Oosterhout (Olanda).

Il prodotto fitosanitario suddetto è registrato al n. 12380.

È approvata quale parte integrante del presente decreto l'etichetta allegata con la quale il prodotto deve essere posto in commercio.

Il presente decreto sarà notificato, in via amministrativa, all'impresa interessata e pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 1° marzo 2013

Il direttore generale: BORRELLO

ALLEGATO

Vivendi® 100

Erbicida selettivo di post–emergenza delle colture di Barbabietola da zucchero, Frumento duro e tenero, Orzo, Avena, Segale, Mais da granella e da foraggio, Cavoli, Cipolla e Colza
Tipo di formulazione: liquido solubile

Vivendi® 100
Composizione
- CLOPYRALID puro g. 9,5 (= 100 g/L)
- Coadiuvanti q.b. a 100

ATTENZIONE MANIPOLARE CON PRUDENZA

CONSIGLI DI PRUDENZA: Conservare fuori dalla portata dei bambini. Conservare lontano da alimenti o mangimi e da bevande. Non mangiare, né bere, né fumare durante l'impiego.

AgriChem B.V., Koopvaardijweg 9, 4906 CV Oosterhout, Olanda
Tel. 00 31 162 431 931 - www.agrichem.com

Officina di produzione: AgriChem B.V., Koopvaardijweg 9, 4906 CV Oosterhout, Olanda

Distribuito da: CEREXAGRI ITALIA S.r.l. (Via Terni, 275 – 47522 S. Carlo di Cesena (FC) – Tel.+39 0547 661523)

Autorizzazione del Ministero della Salute n. del

Taglie: L 1 - 5 - 10 - 20 **Partita n.:**

PRESCRIZIONI SUPPLEMENTARI: Conservare la confezione ben chiusa. Dopo la manipolazione ed in caso di contaminazione lavarsi accuratamente con acqua e sapone. È obbligatorio l'uso di occhiali nella preparazione ed impiego della soluzione diserbante. Il formulato contiene una sostanza attiva tossica per gli organismi acquatici. Osservare scrupolosamente le dosi e le modalità d'impiego indicate. Per proteggere le piante non bersaglio rispettare una fascia di sicurezza non trattata di 5 m dalle zone coltivate. In caso di interruzione della coltivazione con perdita del raccolto attendere almeno 125 giorni dal trattamento prima di effettuare la semina di una nuova coltura. Non contaminare altre colture, alimenti, bevande e corsi d'acqua. Non contaminare l'acqua con il prodotto o il suo contenitore.

INFORMAZIONI PER IL MEDICO: in caso di intossicazione, chiamare il medico per i consueti interventi di pronto soccorso.

CARATTERISTICHE E MODALITÀ D'IMPIEGO
Il Vivendi 100 è un erbicida di post - emergenza della coltura e della infestante, dotato di azione sistemica attraverso le radici e l'apparato fogliare delle infestanti; possiede elevata selettività e viene traslocato rapidamente all'interno delle infestanti.
Viene indicato per combattere :
Daucus carota, Matricaria spp., *Picris echioides, Rumex* spp., *Scandix pecten - veneris, Senecio vulgaris, Sonchus* spp., *Vicia sativa, Xanthium italicum, Artemisia vulgaris, Cirsium arvense, Tussilago farfara, Ammi majus, Anthemis* spp., *Bifora* spp., *Centaurea cyanus, Chrysanthemum segetum, Trifolium* spp., azione parziale su *Poligonum persicaria, Poligonum aviculare* e *Solanum nigrum*.
Colture protette:
BARBABIETOLA DA ZUCCHERO
Si deve intervenire ai primi stadi di sviluppo delle infestanti, con presenza prevalente di *Cirsium arvense*, trattare alla dose di 0,8 - 1 L /ha; se invece vi è prevalenza di *Matricaria chamomilla* la dose deve essere elevata a 1,2 - 1,5 L/ha.
Per completare lo spettro d'azione del prodotto, può essere impiegato in miscela con prodotti a base di Fenmedifam.
FRUMENTO DURO e TENERO - ORZO - AVENA - SEGALE
Si deve intervenire nella fase compresa tra l'accestimento e la fase di botticella della coltura alla dose di 0,8 - 1 L/ha, preferibilmente in miscela con un erbicida ormonico sotto forma di sale e non di estere.
MAIS DA GRANELLA e DA FORAGGIO
Si deve trattare in post - emergenza, con la coltura alta da 15 a 30 cm, alla dose di 0,8 - 1 L/ha.
CAVOLI - CIPOLLA - COLZA
Trattare in post - emergenza alla dose di 1,2 - 1,5 L/ha.

COMPATIBILITÀ: Non compatibile con prodotti a reazione alcalina.

AVVERTENZA: In caso di miscela con altri formulati deve essere rispettato il periodo di carenza più lungo. Devono inoltre essere osservate le norme precauzionali prescritte per i prodotti più tossici. Qualora si verificassero casi di intossicazione, informare il medico della miscelazione compiuta.

FITOTOSSICITÀ: il prodotto può essere fitotossico per le colture non indicate in etichetta.

Sospendere i trattamenti 45 giorni prima della raccolta del mais.

ATTENZIONE: Da impiegarsi esclusivamente per gli usi e alle condizioni riportate in questa etichetta. Chi impiega il prodotto è responsabile degli eventuali danni derivanti da uso improprio del preparato. Il rispetto di tutte le indicazioni contenute nella presente etichetta è condizione essenziale per assicurare l'efficacia del trattamento e per evitare danni alle piante, alle persone ed agli animali. Non applicare con i mezzi aerei. Per evitare rischi per l'uomo e per l'ambiente seguire le istruzioni per l'uso (art. 9, comma 3, D. L.vo n. 65/2003). Operare in assenza di vento. Da non vendersi sfuso. Smaltire le confezioni secondo le norme vigenti. Il contenitore completamente svuotato non deve essere disperso nell'ambiente. Il contenitore non può essere riutilizzato.

1 MAR. 2013
Etichetta autorizzata con decreto dirigenziale del

13A06326

DECRETO 12 marzo 2013.

Modifica dei decreti relativi alla immissione in commercio dei prodotti fitosanitari Fungiben Combi, e Mosaiko Combi, ora modificati nella classificazione ed etichettatura.

IL DIRETTORE GENERALE
PER L'IGIENE E LA SICUREZZA DEGLI ALIMENTI
E LA NUTRIZIONE

Vista l'autorizzazione all'immissione in commercio del prodotto fitosanitario Fungiben Combi, reg. n. 10690, con decreto del 31 gennaio 2001, modificato successivamente con decreti di cui l'ultimo in data 28 giugno 2012;

Vista l'autorizzazione all'immissione in commercio del prodotto fitosanitario Mosaiko Combi, reg. n. 15509, con decreto in data 15 ottobre 2012, uguale al prodotto di riferimento sopra citato;

Visto il regolamento (CE) n. 1272/2008 del Parlamento Europeo e del Consiglio del 16 dicembre 2008 e il successivo regolamento n. 790/2009 della Commissione del 10 agosto 2009 di adeguamento al progresso tecnico e scientifico, relativi alla classificazione, all'etichettatura e all'imballaggio delle sostanze e delle miscele;

Rilevato che nelle etichette dei sopra citati prodotti è riportata una classificazione diversa da quella autorizzata con decreto 14 ottobre 2010 relativo all'adeguamento al sopra citato Reg. 790 del 2009;

Ritenuto di dover modificare le etichette dei prodotti fitosanitari in questione, relativamente alla loro classificazione;

Decreta:

È autorizzata la variazione del testo delle etichette, relativamente alla loro classificazione,dei prodotti fitosanitari FUNGIBEN COMBI, reg. n. 10690, e MOSAIKO COMBI, reg. n. 15509, a nome dell'Impresa Cheminova Agro Italia srl, con sede legale in Bergamo, via F.lli Bronzetti 32/28, preparati negli stabilimenti e nelle taglie già autorizzate.

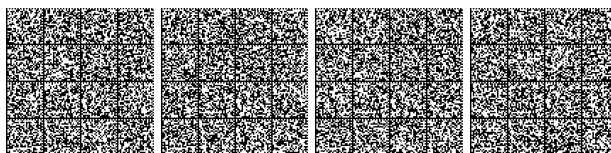
Entro 30 giorni dalla notifica del presente decreto, il titolare dell'autorizzazione è tenuto a rietichettare il prodotto fitosanitario non ancora immesso in commercio e a fornire ai rivenditori un facsimile della nuova etichetta per le confezioni di prodotto giacenti presso gli esercizi di vendita al fine della sua consegna all'acquirente/utilizzatore finale. È altresì tenuto ad adottare ogni iniziativa, nei confronti degli utilizzatori, idonea ad assicurare un corretto impiego del prodotto fitosanitario in conformità alle nuove disposizioni.

È approvata quale parte integrante del presente decreto le etichette allegate con la quale i prodotti devono essere posti in commercio.

Il presente decreto sarà notificato, in via amministrativa, all'Impresa interessata e pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 12 marzo 2013

Il direttore generale: BORRELLO

ALLEGATO

ETICHETTA/FOGLIO ILLUSTRATIVO

Mosaiko Combi

Fungicida sistemico

Polvere bagnabile

MOSAIKO COMBI Registrazione del Ministero della Salute n del

Composizione:
100 grammi di prodotto contengono:

Miclobutanil puro	**g 0,8**
Zolfo puro (esente da selenio)	**g 50**
Coformulanti q.b. a	**g 100**

Cheminova Agro Italia S.r.l.
Via F.lli Bronzetti 32/28 - 24124 Bergamo

Distribuito da:
GOWAN Italia S.p.A. Via Morgagni, 68 - 48018 Faenza (RA)
Tel. 0546 629911

IRRITANTE

Stabilimento di produzione: **S.T.I. - Solfotecnica Italiana S.p.A. - Cotignola (RA)**

Contenuto netto: **g 50 100 250 500; kg 1 5 10 25** **Partita n.....**

FRASI DI RISCHIO: Irritante per la pelle. Nocivo per gli organismi acquatici, può provocare a lungo termine effetti negativi per l'ambiente acquatico.

CONSIGLI DI PRUDENZA: Conservare fuori della portata dei bambini. Conservare lontano da alimenti, mangimi e da bevande. Non mangiare, né bere, né fumare durante l'impiego. Evitare il contatto con la pelle. Usare indumenti protettivi e guanti adatti. In caso d'ingestione consultare immediatamente il medico e mostrargli il contenitore o l'etichetta. Non disperdere nell'ambiente. Riferirsi alle istruzioni speciali/ schede informative in materia di sicurezza.

PRESCRIZIONI SUPPLEMENTARI: Non contaminare l'acqua con il prodotto o il suo contenitore. Non pulire il materiale d'applicazione in prossimità delle acque di superficie. Evitare la contaminazione attraverso i sistemi di scolo delle acque dalle aziende agricole e dalle strade.

INFORMAZIONI PER IL MEDICO
Trattasi di associazione delle seguenti sostanze attive: Miclobutanil 0,8% e Zolfo 50% le quali, separatamente, provocano i seguenti sintomi di intossicazione:
MICLOBUTANIL: Sintomi - organi interessati: occhi, cute, mucosa del tratto respiratorio, fegato, reni. Provoca gravi lesioni cutanee su base allergica (da semplici dermatiti eritematose a dermatiti necrotizzanti). Provoca tosse, broncospasmo e dispnea per irritazione bronchiale. Fenomeni di tossicità sistemica solo per assorbimento di alte dosi. Sono possibili tubulonecrosi renale acuta ed epatonecrosi attribuiti ad un meccanismo immunoallergico. In caso di ingestione insorgono sintomi di gastroenterite (nausea, vomito, diarrea) e cefalea, oltre naturalmente a segni del possibile interessamento epatico e/o renale. Nell'intossicazione grave si evidenziano segni di eccitamento e depressione del SNC. Metabolismo: dopo ingestione la sostanza è prontamente assorbita e metabolizzata. L'escrezione renale e fecale avviene in 72 ore.
ZOLFO: --
Terapia: sintomatica
Avvertenza: Consultare un Centro Antiveleni

CARATTERISTICHE

MOSAIKO COMBI è un fungicida ad azione sistemica e di contatto che associa in maniera ottimale le caratteristiche fitoiatriche dei due principi attivi. Esplica attività anticrittogamica nei confronti dell'oidio della vite, del melo, del pesco e delle cucurbitacee, nonchè nei confronti del Marciume nero (Black-rot)della vite e la Ticchiolatura del melo.

MODALITÀ E DOSI D'IMPIEGO

- VITE:
  - contro l'oidio (*Oidium tuckerii*): impiegare 200 - 350 g/hl con un intervallo di 14 giorni a secondo della pressione della malattia e della sensibilità varietale.
  - contro il marciume nero (*Guignardia bidwellii*): impiegare 250 - 300 g/hl con intervalli di 10 - 14 giorni
- PESCO (COMPRESE NETTARINE E PERCOCHE):
  contro oidio (*Sphaerotheca pannosa*) impiegare 400 g/hl dalla scamiciatura del frutto, ogni 10-14 giorni
- MELO:
  - contro Oidio, impiegare 350 - 400 g/hl con un intervallo di 7-14 giorni in funzione dello sviluppo vegetativo e della pressione della malattia. Il prodotto ha azione cosmetica nei confronti delle varietà sensibili alla rugginosità del frutto.
  - contro Ticchiolatura impiegare 450 g/hl in miscela con un fungicida di contatto.
- MELONE, COCOMERO, ZUCCHINO, CETRIOLO:
  contro oidio (*Erisiphe cichoracearum*) impiegare 400 g/hl intervenendo dalla prima comparsa della malattia ad intervalli di 8-10 giorni. Non impiegare in coltura sotto serra o tunnel, in quanto lo zolfo potrebbe provocare fitotossicità.

COMPATIBILITÀ

AVVERTENZE: In caso di miscela con altri formulati deve essere rispettato il periodo di carenza più lungo. Devono essere inoltre osservate le norme precauzionali prescritte per i prodotti più tossici. Qualora si verificassero casi di intossicazione, informare il medico della miscelazione compiuta.

Sospendere i trattamenti:
7 giorni prima della raccolta su melone, cocomero, zucchino, cetriolo
15 giorni prima della raccolta sulle altre colture

ATTENZIONE

Da impiegarsi esclusivamente per gli usi e alle condizioni riportate in questa etichetta. Chi impiega il prodotto è responsabile degli eventuali danni derivanti da uso improprio del preparato. Il rispetto di tutte le indicazioni contenute nella presente etichetta è condizione essenziale per assicurare l'efficacia del trattamento e per evitare danni alle piante, alle persone ed agli animali.

NON APPLICARE CON MEZZI AEREI
PER EVITARE RISCHI PER L'UOMO E PER L'AMBIENTE SEGUIRE LE ISTRUZIONI PER L'USO
NON CONTAMINARE ALTRE COLTURE, ALIMENTI E BEVANDE O CORSI D'ACQUA
OPERARE IN ASSENZA DI VENTO
DA NON VENDERSI SFUSO
SMALTIRE LE CONFEZIONI SECONDO LE NORME VIGENTI
IL CONTENITORE COMPLETAMENTE SVUOTATO NON DEVE ESSERE DISPERSO NELL'AMBIENTE
IL CONTENITORE NON PUÒ ESSERE RIUTILIZZATO

Etichetta autorizzata con decreto dirigenziale del 12 MAR. 2013

ETICHETTA FORMATO RIDOTTO

Mosaiko Combi

Fungicida sistemico

Polvere bagnabile

MOSAIKO COMBI Registrazione del Ministero della Salute n del

Composizione:
100 grammi di prodotto contengono:

Miclobutanil puro	**g 0,8**
Zolfo puro (esente da selenio)	**g 50**
Coformulanti q.b. a	**g 100**

IRRITANTE

Cheminova Agro Italia S.r.l.
Via F.lli Bronzetti 32/28 - 24124 Bergamo

Contenuto netto: **g 50 100** Partita n.....

Distribuito da:
GOWAN Italia S.p.A. Via Morgagni, 68 - 48018 Faenza (RA) Tel. 0546 629911
Stabilimento di produzione: **S.T.I. - Solfotecnica Italiana S.p.A. - Cotignola (RA)**
FRASI DI RISCHIO: Irritante per la pelle. Nocivo per gli organismi acquatici, può provocare a lungo termine effetti negativi per l'ambiente acquatico.
CONSIGLI DI PRUDENZA: Conservare fuori della portata dei bambini. Conservare lontano da alimenti, mangimi e da bevande. Non mangiare, né bere, né fumare durante l'impiego. Evitare il contatto con la pelle. Usare indumenti protettivi e guanti adatti. In caso d'ingestione consultare immediatamente il medico e mostrargli il contenitore o l'etichetta. Non disperdere nell'ambiente. Riferirsi alle istruzioni speciali/ schede informative in materia di sicurezza.

PRIMA DELL'USO LEGGERE IL FOGLIO ILLUSTRATIVO

SMALTIRE LE CONFEZIONI SECONDO LE NORME VIGENTI
IL CONTENITORE NON PUÒ ESSERE RIUTILIZZATO
IL CONTENITORE COMPLETAMENTE SVUOTATO NON DEVE ESSERE DISPERSO NELL'AMBIENTE

Etichetta autorizzata con decreto dirigenziale del .... 12 MAR. 2013

ETICHETTA/FOGLIO ILLUSTRATIVO

FUNGIBEN COMBI Registrazione n. 10690 Ministero della Sanità del 31/01/2001

Composizione:	
100 grammi di prodotto contengono:	
Miclobutanil puro	g 0,8
Zolfo puro (esente da selenio)	g 50
Coformulanti q.b. a	g 100

IRRITANTE

Cheminova Agro Italia S.r.l.
Via F.lli Bronzetti 32/28 - 24124 Bergamo
Tel 035 19904468

Contenuto netto: **g 50 100 250 500; kg 1 5 10 25**

Officina di produzione: S.T.I. - **Solfotecnica Italiana S.p.A. - Cotignola (RA)**
Officina di confezionamento: **Torre srl – Torrenieri (SI)**

Partita n.*

FRASI DI RISCHIO: Irritante per la pelle. Nocivo per gli organismi acquatici, può provocare a lungo termine effetti negativi per l'ambiente acquatico.

CONSIGLI DI PRUDENZA: Conservare fuori della portata dei bambini. Conservare lontano da alimenti, mangimi e da bevande. Non mangiare, né bere, né fumare durante l'impiego. Evitare il contatto con la pelle. Usare indumenti protettivi e guanti adatti. In caso d'ingestione consultare immediatamente il medico e mostrargli il contenitore o l'etichetta. Non disperdere nell'ambiente. Riferirsi alle istruzioni speciali/ schede informative in materia di sicurezza.

PRESCRIZIONI SUPPLEMENTARI

Non contaminare l'acqua con il prodotto o il suo contenitore. Non pulire il materiale d'applicazione in prossimità delle acque di superficie. Evitare la contaminazione attraverso i sistemi di scolo delle acque dalle aziende agricole e dalle strade.

INFORMAZIONI PER IL MEDICO

Trattasi di associazione delle seguenti sostanze attive: Miclobutanil 0,8% e Zolfo 50% le quali, separatamente, provocano i seguenti sintomi di intossicazione:

MICLOBUTANIL: Sintomi - organi interessati: occhi, cute, mucosa del tratto respiratorio, fegato, reni. Provoca gravi lesioni cutanee su base allergica (da semplici dermatiti eritematose a dermatiti necrotizzanti). Provoca tosse, broncospasmo e dispnea per irritazione bronchiale. Fenomeni di tossicità sistemica solo per assorbimento di alte dosi. Sono possibili tubulonecrosi renale acuta ed epatonecrosi attribuiti ad un meccanismo immunoallergico. In caso di ingestione insorgono sintomi di gastroenterite (nausea, vomito, diarrea) e cefalea, oltre naturalmente a segni del possibile interessamento epatico e/o renale. Nell'intossicazione grave si evidenziano segni di eccitamento e depressione del SNC. Metabolismo: dopo ingestione la sostanza è prontamente assorbita e metabolizzata. L'escrezione renale e fecale avviene in 72 ore.

ZOLFO: --

Terapia: sintomatica

Avvertenza: Consultare un Centro Antiveleni

CARATTERISTICHE

FUNGIBEN COMBI è un fungicida ad azione sistemica e di contatto che associa in maniera ottimale le caratteristiche fitoiatriche dei due principi attivi. Esplica attività anticrittogamica nei confronti dell'oidio della vite, del melo, del pesco e delle cucurbitacee, nonché nei confronti del Marciume nero (Black-rot)della vite e la Ticchiolatura del melo.

MODALITÀ E DOSI D'IMPIEGO

- VITE:
  - contro l'oidio (*Oidium tuckerii*): impiegare 200-350 g/hl con un intervallo di 14 giorni a secondo della pressione della malattia e della sensibilità varietale.
  - contro il marciume nero (*Guignardia bidwellii*): impiegare 250-300 g/hl con intervalli di 10-14 giorni
- PESCO (COMPRESE NETTARINE E PERCOCHE):
  contro oidio (*Sphaerotheca pannosa*) impiegare 400 g/hl dalla scamiciatura del frutto, ogni 10-14 giorni
- MELO:
  - contro Oidio, impiegare 350-400 g/hl con un intervallo di 7-14 giorni in funzione dello sviluppo vegetativo e della pressione della malattia. Il prodotto ha azione cosmetica nei confronti delle varietà sensibili alla rugginosità del frutto.
  - contro Ticchiolatura impiegare 450 g/hl in miscela con un fungicida di contatto.
- MELONE, COCOMERO, ZUCCHINO, CETRIOLO:
  contro oidio (*Erisiphe cichoracearum*) impiegare 400 g/hl intervenendo dalla prima comparsa della malattia ad intervalli di 8-10 giorni. Non impiegare in coltura sotto serra o tunnel, in quanto lo zolfo potrebbe provocare fitotossicità.

COMPATIBILITÀ

AVVERTENZE: In caso di miscela con altri formulati deve essere rispettato il periodo di carenza più lungo. Devono essere inoltre osservate le norme precauzionali prescritte per i prodotti più tossici. Qualora si verificassero casi di intossicazione, informare il medico della miscelazione compiuta.

Sospendere i trattamenti:
7 giorni prima della raccolta su melone, cocomero, zucchino, cetriolo
15 giorni prima della raccolta sulle altre colture

ATTENZIONE
Da impiegarsi esclusivamente per gli usi e alle condizioni riportate in questa etichetta.
Chi impiega il prodotto è responsabile degli eventuali danni derivanti da uso improprio del preparato.
Il rispetto di tutte le indicazioni contenute nella presente etichetta è condizione essenziale per assicurare l'efficacia del trattamento e per evitare danni alle piante, alle persone ed agli animali.
NON APPLICARE CON MEZZI AEREI
PER EVITARE RISCHI PER L'UOMO E PER L'AMBIENTE SEGUIRE LE ISTRUZIONI PER L'USO
NON CONTAMINARE ALTRE COLTURE, ALIMENTI E BEVANDE O CORSI D'ACQUA
OPERARE IN ASSENZA DI VENTO
DA NON VENDERSI SFUSO
SMALTIRE LE CONFEZIONI SECONDO LE NORME VIGENTI
IL CONTENITORE COMPLETAMENTE SVUOTATO NON DEVE ESSERE DISPERSO NELL'AMBIENTE
IL CONTENITORE NON PUÒ ESSERE RIUTILIZZATO

Etichetta autorizzata con decreto dirigenziale del 12 MAR. 2013

Etichetta formato ridotto

Fungiben Combi

Fungicida sistemico

Polvere bagnabile

FUNGIBEN COMBI Registrazione n. 10690 Ministero della Sanità del 31/01/2001

Composizione:
100 grammi di prodotto contengono:

Miclobutanil puro	**g 0,8**
Zolfo puro (esente da selenio)	**g 50**
Coformulanti q.b. a	**g 100**

Cheminova Agro Italia S.r.l.
Via F.lli Bronzetti 32/28 - 24124 Bergamo
Tel 035 19904468

Contenuto netto: **g 50-100** Partita n.*

IRRITANTE

Officina di produzione: S.T.I. - **Solfotecnica Italiana S.p.A. - Cotignola (RA)**
Officina di confezionamento: **Torre srl – Torrenieri (SI)**
FRASI DI RISCHIO: Irritante per la pelle. Nocivo per gli organismi acquatici, può provocare a lungo termine effetti negativi per l'ambiente acquatico.
CONSIGLI DI PRUDENZA: Conservare fuori della portata dei bambini. Conservare lontano da alimenti, mangimi e da bevande. Non mangiare, né bere, né fumare durante l'impiego. Evitare il contatto con la pelle. Usare indumenti protettivi e guanti adatti. In caso d'ingestione consultare immediatamente il medico e mostrargli il contenitore o l'etichetta. Non disperdere nell'ambiente. Riferirsi alle istruzioni speciali/ schede informative in materia di sicurezza.

PRIMA DELL'USO LEGGERE IL FOGLIO ILLUSTRATIVO
SMALTIRE LE CONFEZIONI SECONDO LE NORME VIGENTI
IL CONTENITORE NON PUÒ ESSERE RIUTILIZZATO
IL CONTENITORE COMPLETAMENTE SVUOTATO NON DEVE ESSERE DISPERSO NELL'AMBIENTE

Etichetta autorizzata con decreto dirigenziale del 12 MAR. 2013

13A06327

MINISTERO DELLE POLITICHE AGRICOLE ALIMENTARI E FORESTALI

DECRETO 3 luglio 2013.

Iscrizione di una varietà nel registro nazionale dei portainnesti di piante ortive.

IL DIRETTORE GENERALE
DELLO SVILUPPO RURALE

Vista la legge 25 novembre 1971, n. 1096, e successive modifiche ed integrazioni, che disciplina l'attività sementiera ed in particolare gli articoli 19 e 24 che prevedono l'istituzione obbligatoria, per ciascuna specie di coltura, dei registri di varietà aventi lo scopo di permettere l'identificazione delle varietà stesse;

Visto il decreto del Presidente della Repubblica 8 ottobre 1973, n. 1065, recante «Regolamento di esecuzione della legge 25 novembre 1971, n. 1096»;

Vista la legge 20 aprile 1976, n. 195, che modifica la citata legge n. 1096/71 ed in particolare gli articoli 4 e 5 che prevedono la suddivisione dei registri di varietà di specie di piante ortive e la loro istituzione obbligatoria;

Visto il decreto ministeriale 17 luglio 1976, che istituisce i registri di varietà di specie di piante ortive;

Visto il decreto legislativo 7 luglio 2011, n. 124, recante attuazione della direttiva 2008/72/CE del Consiglio del 15 luglio 2008, relativa alla commercializzazione delle piantine di ortaggi e dei materiali di moltiplicazione di ortaggi ad eccezione delle sementi, ed in particolare l'art. 8, comma 1 c, secondo cui le piantine di ortaggi ed i materiali di moltiplicazione di ortaggi, ad eccezione delle sementi, possono essere commercializzati soltanto se fanno riferimento ad una varietà ufficialmente iscritta;

Visto il decreto ministeriale del 15 giugno 2012, n. 13094, che istituisce il registro nazionale dei portainnesti di piante ortive;

Visto in particolare l'art. 3, comma 2, del citato D.M. n. 13094 del 15 giugno 2012, secondo il quale, in assenza dei criteri di iscrizione di tali varietà, da stabilirsi con successivo provvedimento, l'iscrizione al registro nazionale delle varietà di portainnesti di piante ortive è effettuata sulla base dei risultati di esami non ufficiali, informazioni pratiche acquisite nel corso della coltivazione o di ogni ulteriore informazione o documentazione ritenuta utile ai fini dell'esame della domanda;

Visto il decreto legislativo 30 luglio 1999, n. 300, di riforma dell'organizzazione di governo a norma dell'art. 11 della legge 15 marzo 1997, n. 59;

Visto il decreto legislativo 30 marzo 2001, n. 165, relativo alle «norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche», in particolare l'art. 4, commi 1 e 2 e l'art. 16, comma 1;

Visto il D.P.R. del 14 febbraio del 2012, n. 41, recante il Regolamento di riorganizzazione del Ministero delle politiche agricole alimentari e forestali;

Visto il decreto del Ministro delle politiche agricole alimentari e forestali n. 12081 del 2 agosto 2012, registrato alla Corte dei conti, recante individuazione degli uffici dirigenziali non generali;

Vista la domanda presentata ai fini dell'iscrizione di una varietà vegetale di portainnesto nel rispettivo registro nazionale;

Ritenuto di dover procedere in conformità;

Decreta:

Articolo unico

Ai sensi dell'art. 1 del decreto ministeriale del 15 giugno 2012, n. 13094, è iscritta nel registro nazionale dei portainnesti di piante ortive la varietà ortiva sotto elencata.

Specie	Varietà	Responsabile della conservazione in purezza
Lagenaria siceraria (Molina) Standley	OL1330	Blumen s.r.l.

Il presente decreto entra in vigore il giorno successivo a quello della pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 3 luglio 2013

Il direttore generale: CACOPARDI

AVVERTENZA:

Il presente atto non è soggetto al visto di controllo preventivo di legittimità da parte della Corte dei conti, art. 3, legge 14 gennaio 1994, n. 20, né alla registrazione da parte dell'Ufficio centrale del bilancio del Ministero dell'economia e delle finanze, art. 9 del decreto del Presidente della Repubblica n. 38/1998.

13A06323

DECRETO 9 luglio 2013.

Iscrizione di varietà ortive nel relativo registro nazionale.

IL DIRETTORE GENERALE
DELLO SVILUPPO RURALE

Vista la legge 25 novembre 1971, n. 1096, e successive modifiche ed integrazioni, che disciplina l'attività sementiera ed in particolare gli articoli 19 e 24 che prevedono l'istituzione obbligatoria, per ciascuna specie di coltura, dei registri di varietà aventi lo scopo di permettere l'identificazione delle varietà stesse;

Visto il decreto del Presidente della Repubblica 8 ottobre 1973, n. 1065, recante "Regolamento di esecuzione della legge 25 novembre 1971, n. 1096";

Vista la legge 20 aprile 1976, n. 195, che modifica la citata legge 1096/71 ed in particolare gli articoli 4 e 5 che prevedono la suddivisione dei registri di varietà di specie di piante ortive e la loro istituzione obbligatoria;

Visto il decreto ministeriale 17 luglio 1976, che istituisce i registri di varietà di specie di piante ortive;

Visto il decreto legislativo 30 luglio 1999, n. 300, di riforma dell'organizzazione di governo a norma dell'art. 11 della legge 15 marzo 1997, n. 59;

Visto il decreto legislativo 30 marzo 2001, n. 165, relativo alle "norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche", in particolare l'art. 4, commi 1 e 2 e l'art. 16, comma 1;

Visto il decreto del Presidente della Repubblica del 14 febbraio del 2012, n. 41, recante il Regolamento di riorganizzazione del Ministero delle politiche agricole alimentari e forestali;

Visto il decreto del Ministro delle politiche agricole alimentari e forestali n. 12081 del 2 agosto 2012, registrato alla Corte dei Conti, recante individuazione degli uffici dirigenziali non generali.

Viste le domande presentate ai fini dell'iscrizione delle varietali vegetali nei rispettivi registri nazionali;

Visti i risultati delle prove condotte per l'accertamento dei requisiti varietali previsti dalla normativa vigente;

Ritenuto di dover procedere in conformità;

Decreta:

Articolo unico

Ai sensi dell'art. 17 del decreto del Presidente della Repubblica 8 ottobre 1973, n. 1065, sono iscritte nel registro delle varietà dei prodotti sementieri, fino alla fine del decimo anno civile successivo la pubblicazione del presente decreto, le varietà di specie ortive sotto elencate, le cui sementi possono essere controllate in quanto "sementi standard" e la cui descrizione e i risultati delle prove eseguite sono depositati presso questo Ministero:

Specie	**Varietà**	**Codice SIAN**	**Lista Registro**	**Ibrido**	**Responsabile della conservazione in purezza**
Melanzana	Niobe	3429	B	H	S.A.I.S. Società Agricola Italiana Sementi
Pomodoro	Sybilla	3430	B	H	S.A.I.S. Società Agricola Italiana Sementi
Pomodoro	Syrio	3431	B	H	S.A.I.S. Società Agricola Italiana Sementi
Pomodoro	Torrano	3433	B	H	S.A.I.S. Società Agricola Italiana Sementi
Peperone	Giubileo	3434	B	H	S.A.I.S. Società Agricola Italiana Sementi

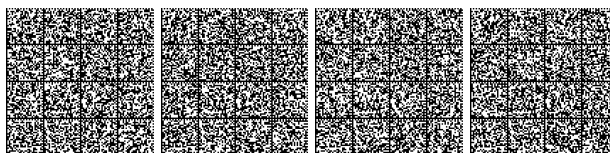
Il presente decreto entra in vigore il giorno successivo a quello della pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 9 luglio 2013

Il direttore generale: CACOPARDI

AVVERTENZA:

Il presente atto non è soggetto al visto di controllo preventivo di legittimità da parte della Corte dei conti, art.3, legge 14 gennaio 1994, n. 20, né alla registrazione da parte dell'Ufficio centrale del bilancio del Ministero dell'economia e delle finanze, art. 9 del decreto del Presidente della Repubblica n. 38/1998

13A06322

DECRETO 9 luglio 2013.

Iscrizione di una varietà ortiva nel relativo registro nazionale.

IL DIRETTORE GENERALE
DELLO SVILUPPO RURALE

Vista la legge 25 novembre 1971, n. 1096, e successive modifiche ed integrazioni, che disciplina l'attività sementiera ed in particolare gli articoli 19 e 24 che prevedono l'istituzione obbligatoria, per ciascuna specie di coltura, dei registri di varietà aventi lo scopo di permettere l'identificazione delle varietà stesse;

Visto il decreto del Presidente della Repubblica 8 ottobre 1973, n. 1065, recante «Regolamento di esecuzione della legge 25 novembre 1971, n. 1096»;

Vista la legge 20 aprile 1976, n. 195, che modifica la citata legge n. 1096/71 ed in particolare gli articoli 4 e 5 che prevedono la suddivisione dei registri di varietà di specie di piante ortive e la loro istituzione obbligatoria;

Visto il decreto ministeriale 17 luglio 1976, che istituisce i registri di varietà di specie di piante ortive;

Visto il decreto legislativo 30 luglio 1999, n. 300, di riforma dell'organizzazione di governo a norma dell'art. 11 della legge 15 marzo 1997, n. 59;

Visto il decreto legislativo 30 marzo 2001, n. 165, relativo alle «norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche», in particolare l'art. 4, commi 1 e 2 e l'art. 16, comma 1;

Visto il D.P.R. del 14 febbraio del 2012, n. 41, recante il Regolamento di riorganizzazione del Ministero delle politiche agricole alimentari e forestali;

Visto il decreto del Ministro delle politiche agricole alimentari e forestali n. 12081 del 2 agosto 2012, registrato alla Corte dei conti, recante individuazione degli uffici dirigenziali non generali;

Vista la domanda presentata ai fini dell'iscrizione della varietà vegetale nel rispettivo registro nazionale;

Visti i risultati delle prove condotte per l'accertamento dei requisiti varietali previsti dalla normativa vigente;

Considerato che l'iscrizione della varietà, nel relativo registro, era stata temporaneamente sospesa per l'espletamento di controlli tecnico-amministrativi della domanda d'iscrizione;

Ritenuto di dover procedere in conformità;

Decreta:

Articolo unico

Ai sensi dell'art. 17 del decreto del Presidente della Repubblica 8 ottobre 1973, n. 1065, è iscritta nel registro delle varietà dei prodotti sementieri, fino alla fine del decimo anno civile successivo la pubblicazione del presente decreto, la varietà ortiva di seguito elencata, le cui sementi possono essere certificate in quanto «sementi di base», «sementi certificate» o controllate in quanto «sementi standard» e la cui descrizione e i risultati delle prove eseguite sono depositati presso questo Ministero:

Specie	Varietà	Codice SIAN	Lista Registro	Ibrido	Responsabile della conservazione in purezza
Pomodoro	Brunilde	2980	A	H	Agriseeds s.r.l.

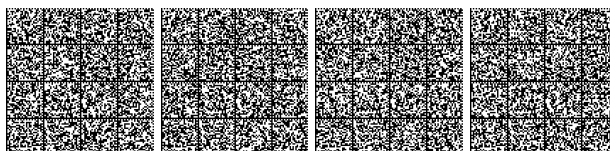
Il presente decreto entra in vigore il giorno successivo a quello della pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 9 luglio 2013

Il direttore generale: CACOPARDI

AVVERTENZA:

Il presente atto non è soggetto al visto di controllo preventivo di legittimità da parte della Corte dei conti, art. 3, legge 14 gennaio 1994, n. 20, né alla registrazione da parte dell'Ufficio centrale del bilancio del Ministero dell'economia e delle finanze, art. 9 del decreto del Presidente della Repubblica n. 38/1998.

13A06324

MINISTERO DELLO SVILUPPO ECONOMICO

DECRETO 9 luglio 2013.

Proroga dell'autorizzazione all'Organismo «Cert. Im. S.r.l.», in Napoli, per lo svolgimento delle attività di verifica periodica e straordinaria di cui agli articoli 13 e 14 del decreto del Presidente della Repubblica 30 aprile 1999, n. 162, di attuazione della direttiva europea 95/16/CE in materia di ascensori.

IL DIRETTORE GENERALE
PER IL MERCATO, LA CONCORRENZA,
IL CONSUMATORE, LA VIGILANZA E LA NORMATIVA TECNICA

Visto il Regolamento (CE) N. 765/2008 del Parlamento europeo e del Consiglio del 9 luglio 2008 che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93;

Vista la Decisione N. 768/2008/CE del Parlamento europeo e del Consiglio del 9 luglio 2008 relativa a un quadro comune per la commercializzazione dei prodotti e che abroga la decisione 93/465/CEE;

Visto l'art. 4 della legge 23 luglio 2009, n. 99 "Disposizioni in materia di sviluppo e internazionalizzazione delle imprese, nonché in materia di energia.", recante disposizioni al fine di assicurare la prontÀ"Attuazione del capo II del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, che pone norme in materia di accreditamento e vigilanza del mercato per la commercializzazione dei prodotti";

Visti il Decreto Legislativo 30 luglio 1999, n. 300 "Riforma dell'organizzazione del Governo, a norma dell'art. 11 della legge 15 marzo 1997, n. 59" e successive modificazioni e integrazioni, ed in particolare gli articoli da 27 a 32 e l'art. 55, recanti norme di istituzione del Ministero delle attività produttive e di trasferimento allo stesso delle funzioni del Ministero dell'industria, del commercio e dell'artigianato, del Ministero del commercio con l'estero, del Dipartimento del turismo istituito presso la Presidenza del Consiglio dei Ministri;

Visto il Decreto-Legge 18 maggio 2006 n. 181 "Disposizioni urgenti in materia di riordino delle attribuzioni della Presidenza del Consiglio dei Ministri e dei Ministeri" convertito in legge, con modificazioni, dalla legge 17 luglio 2006, n. 233, in particolare l'art. 1, comma 12 con cui la denominazione «Ministero dello sviluppo economico» sostituisce, ad ogni effetto e ovunque presente, la denominazione «Ministero delle attività produttive»;

Vista la Direttiva 95/16/CE del Parlamento Europeo e del Consiglio del 29 giugno 1995 per il ravvicinamento delle legislazioni degli Stati Membri relative agli ascensori;

Visto il Decreto del Presidente della Repubblica 30 aprile 1999, n. 162 "Regolamento recante norme per l'attuazione della Direttiva 95/16/CE sugli ascensori e di semplificazione dei procedimenti per la concessione del nulla osta per ascensori e montacarichi, nonché della relativa licenza di esercizio", pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana n. 134 del 10 giugno 1999;

Visto il Decreto del Presidente della Repubblica 5 ottobre 2010, n. 214, concernente il "Regolamento recante modifiche al Decreto del Presidente della Repubblica 30 aprile 1999, n. 162, per la parziale attuazione della Direttiva 2006/42/CE relativa alle macchine e che modifica la Direttiva 95/16/CE relativa agli ascensori", pubblicato nella *Gazzetta Ufficiale* n. 292 del 15 dicembre 2010;

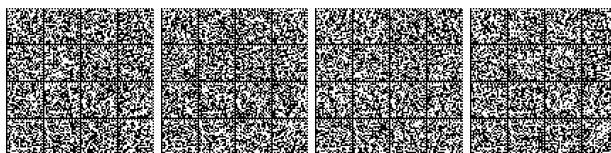
Visto il Decreto 22 dicembre 2009 "Prescrizioni relative all'organizzazione ed al funzionamento dell'unico organismo nazionale italiano autorizzato a svolgere attività di accreditamento in conformità al regolamento (CE) n. 765/2008.";

Visto il Decreto 22 dicembre 2009 "Designazione di «Accredia» quale unico organismo nazionale italiano autorizzato a svolgere attività di accreditamento e vigilanza del mercato.";

Vista la Convenzione, del 22 giugno 2011, ed in particolare l'art. 3, secondo cui il Ministero dello Sviluppo Economico e il Ministero del Lavoro e delle Politiche Sociali hanno affidato all'Organismo Nazionale Italiano di Accreditamento -ACCREDIA- il compito di rilasciare accreditamenti in conformità alle norme UNI CEI EN ISO IEC 17020, 17021, 17024, 17025, UNI CEI EN 45011 e alle Guide europee di riferimento, ove applicabili, agli Organismi incaricati di svolgere attività di valutazione della conformità ai requisiti essenziali di sicurezza, di quattro direttive e nella fattispecie, della Direttiva 95/16/CE del Parlamento europeo e del Consiglio del 29 giugno 1995 per il ravvicinamento delle legislazioni degli Stati membri relative agli ascensori;

Vistal'istanza dell'Organismo CERT. IM. S.R.L. di proroga dell'autorizzazione ministeriale allo svolgimento delle attività di verifica periodica e straordinaria, di cui agli articoli 13 e 14 del decreto del Presidente della Repubblica 162/1999, e relativa integrazione, acquisita agli atti della Direzione generale con rispettivi numeri di protocollo: 106345 del 25/06/2013 e 109122 del 28/06/2013;

Acquisito che l'Organismo citato ha presentato ad ACCREDIA domanda di accreditamento per la certificazione CE degli ascensori e per gli articoli 13 e 14 di cui al Decreto del Presidente della Repubblica 30 aprile 1999, n. 162 citato;

Considerato che i tempi di espletamento dell'attività di ACCREDIA non consentono il rilascio da parte di questo Ministero del decreto di autorizzazione, in modo da non determinare soluzione di continuità con l'autorizzazione scaduta;

Considerato, altresì, l'esame documentale relativo eseguito dall'Ente unico di accreditamento e la dichiarazione (DC2013UTL365 del 14 giugno 2013- Prot. MISE n. 101346 del 17/06/2013) da parte del medesimo Ente, attestante che l'Organismo, nelle more del completamento dell'*iter* di accreditamento, è organizzato per eseguire le attività di verifica di cui agli articoli 13 e 14 del citato decreto del Presidente della Repubblica n.162/99.

Considerato che, nel periodo di vigenza delle precedenti autorizzazioni, non sono stati formulati rilievi di inadeguatezza delle capacità tecniche e professionali, né è stata constatata la mancata osservanza dei criteri minimi, fissati nell'allegato VII del Decreto del Presidente della Repubblica 30 aprile 1999 n. 162;

Ritenuto opportuno consentire all'Organismo sopra citato di continuare le attività specificate all'art. 1 del presente decreto per tutto il tempo necessario all'ottenimento dell'accreditamento da parte di Accredia;

Sentito il Ministero del Lavoro e delle Politiche Sociali, in ottemperanza al disposto di cui all'art. 9, comma 2 del Decreto del Presidente della Repubblica 30 aprile 1999, n. 162.

Decreta:

Art. 1.

1. L'Organismo CERT. IM. S.R.L., nel sito operativo di Centro Direzionale F11 – 80143 Napoli, è autorizzato ad effettuare attività di verifica in conformità a quanto previsto dagli articoli 13 e 14 del decreto del Presidente della Repubblica n. 162/99.

2. La presente autorizzazione ha validità fino alla data del 31 dicembre 2013.

Il presente decreto di autorizzazione è pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana ed è efficace dalla notifica al soggetto destinatario del provvedimento.

Roma, 9 luglio 2013

Il direttore generale: VECCHIO

13A06328

ESTRATTI, SUNTI E COMUNICATI

BANCA D'ITALIA

Nuove disposizioni di vigilanza prudenziale per le banche - Circolare n. 263 del 27 dicembre 2006 - 15° aggiornamento del 2 luglio 2013.

Con il presente aggiornamento sono inseriti nel Titolo V della Circolare n. 263 del 27 dicembre 2006 «Nuove disposizioni di vigilanza prudenziale per le banche» il Capitolo 7 «Il sistema dei controlli interni», il Capitolo 8 «Il sistema informativo» e il Capitolo 9 «La continuità operativa».

Il Capitolo 7 definisce un quadro organico di principi e regole cui deve essere ispirato il sistema dei controlli interni, senza tuttavia esaurire le disposizioni organizzative applicabili alle banche. Le disposizioni ivi contenute, infatti, rappresentano la cornice di riferimento nella quale si inquadrano le regole sui controlli dettate all'interno di specifici ambiti disciplinari (ad es., regole organizzative in materia di gestione di singoli profili di rischio, di sistemi interni di misurazione dei rischi per il calcolo dei requisiti patrimoniali, di processo ICAAP, di prevenzione del rischio di riciclaggio) (c.d. modello «*hub and spokes*»).

Le disposizioni introducono alcune novità di rilievo rispetto al vigente quadro normativo, al fine di dotare le banche di un sistema dei controlli interni completo, adeguato, funzionale e affidabile.

In particolare, le nuove norme enfatizzano il ruolo dell'organo con funzione di supervisione strategica nella definizione del modello di *business* e del *Risk Appetite Framework*; a tale organo è richiesto anche di favorire la diffusione di una cultura dei controlli attraverso l'approvazione di un codice etico al quale sono tenuti a uniformarsi i componenti degli organi aziendali e i dipendenti.

All'organo con funzione di gestione è invece richiesto di avere un'approfondita comprensione di tutti i rischi aziendali e, nell'ambito di una gestione integrata, delle loro interrelazioni reciproche e con l'evoluzione del contesto esterno (incluso il rischio macroeconomico).

Le disposizioni richiedono ai vertici delle banche di porre particolare attenzione alla definizione delle politiche e dei processi aziendali di maggiore rilievo, quali quelli riguardanti: la gestione dei rischi; la valutazione delle attività aziendali; l'approvazione di nuovi prodotti/servizi o dell'avvio di nuove attività nonché dell'inserimento in nuovi mercati; lo sviluppo e la convalida dei modelli interni di misurazione dei rischi non utilizzati a fini regolamentari.

La disciplina delle funzioni aziendali di controllo (*internal audit, compliance e risk management*) è stata profondamente rivisitata; in particolare:

— la nomina e la revoca dei responsabili delle funzioni aziendali di controllo sono di competenza esclusiva dell'organo con funzione di supervisione strategica, sentito l'organo con funzione di controllo;

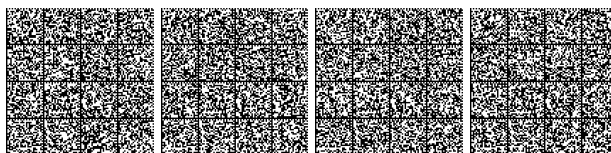
— i responsabili della funzione di controllo dei rischi (c.d. *Chief Risk Officer*) e della funzione di conformità alle norme sono posti, almeno, alle dipendenze dell'organo con funzione di gestione, ferma restando la loro prerogativa di avere accesso diretto all'organo con funzione di supervisione strategica e all'organo con funzione di controllo. Il responsabile della funzione di revisione interna è, invece, sempre collocato a riporto gerarchico dell'organo con funzione di supervisione strategica;

— le tre funzioni aziendali di controllo sono indipendenti dalle aree di *business* e fra loro separate. Se coerente con il principio di proporzionalità, è consentito alle banche di istituire un'unica funzione di conformità alle norme e di controllo dei rischi, ferma restando l'esigenza di mantenere in ogni caso separata la funzione di revisione interna per assicurare l'imparzialità dei controlli di *audit* sulle altre funzioni di controllo;

— i poteri della funzione di *risk management* sono stati rafforzati. La funzione, oltre a collaborare alla definizione del RAF, è chiamata, tra l'altro, a fornire pareri preventivi sulla coerenza delle operazioni di maggiore rilievo con il RAF stesso. In caso di parere negativo, la decisione sull'operazione è rimessa all'organo con funzione di gestione;

— nell'ambito della disciplina sulla conformità alle norme — fermo restando che il presidio sul rischio di non conformità svolto dalla funzione di *compliance* si riferisce a tutte le disposizioni applicabili alle banche, incluse quelle di natura fiscale — il coinvolgimento della funzione è graduato in relazione sia al rilievo che le singole norme hanno per l'attività svolta e per le conseguenze della loro violazione sia all'esistenza all'interno della banca di altre forme di presidio specializzato a fronte del rischio di non conformità relativo a specifiche normative.

Per assicurare il coordinamento e l'interazione tra le varie funzioni e organi con compiti di controllo (previsti dalla normativa societaria, contabile o di vigilanza), l'organo con funzione di supervisione strategica approva uno specifico documento in cui sono precisati compiti, responsabilità e modalità di coordinamento/collaborazione tra le varie funzioni di controllo coinvolte.

È stata, poi, introdotta una disciplina organica in materia di esternalizzazione. Le banche sono tenute a presidiare attentamente i rischi

derivanti dall'esternalizzazione, mantenendo la capacità di controllo e la responsabilità delle attività esternalizzate nonché le competenze essenziali per re-internalizzare le stesse in caso di necessità. Disposizioni specifiche riguardano le condizioni per esternalizzare funzioni aziendali importanti o di controllo. Requisiti meno stringenti sono invece previsti nel caso di esternalizzazione all'interno di un gruppo bancario. Due specifici procedimenti amministrativi sono stati definiti per il divieto dell'esternalizzazione di funzioni operative importanti o di controllo, rispettivamente, al di fuori o all'interno del gruppo bancario (*cfr.* Sezioni IV e V); tali procedimenti integrano il Provvedimento del 25 giugno 2008, in materia di individuazione dei termini e delle unità organizzative responsabili dei procedimenti amministrativi di competenza della Banca d'Italia.

Il Capitolo 8 contiene la disciplina del sistema informativo che è stata integralmente rivista, anche per recepire le principali evoluzioni emerse nel panorama internazionale. Sono stati, tra l'altro, disciplinati: la *governance* e l'organizzazione del sistema informativo; la gestione del rischio informatico; i requisiti per assicurare la sicurezza informatica e il sistema di gestione dei dati. Le disposizioni, inoltre, prevedono che nella definizione dei presidi di sicurezza per l'accesso a sistemi e servizi critici tramite il canale internet trovino applicazione le Raccomandazioni della BCE in materia di sicurezza dei pagamenti in internet.

Il Capitolo 9 disciplina la materia della continuità operativa, riorganizzando le disposizioni attualmente contenute in diverse fonti. Tra le novità di maggiore rilievo, vi è la formalizzazione del ruolo del CODISE, struttura per il coordinamento della gestione delle crisi operative della piazza finanziaria italiana presieduta dalla Banca d'Italia. Inoltre, è stato definito un processo di rapida escalation da incidente a emergenza in modo da assicurare che la dichiarazione dello stato di crisi avvenga nel minor tempo possibile dalla rilevazione dell'incidente. Il tempo complessivo di ripristino non dovrà superare le quattro ore, inclusi i tempi per le fasi di analisi, decisionali, intervento tecnico e verifica.

Le presenti disposizioni sono state sottoposte a consultazione pubblica e ad analisi di impatto della regolamentazione. Nel sito internet della Banca d'Italia sono pubblicati il resoconto della consultazione, la relazione sull'analisi di impatto e le osservazioni pervenute nella fase di consultazione.

Il presente aggiornamento entra in vigore il giorno di pubblicazione sul sito internet della Banca d'Italia.

Le banche si conformano alle disposizioni contenute nel Capitolo 7 (*Il sistema dei controlli interni*) entro il 1° luglio 2014 (data di efficacia), fatto salvo quanto segue:

— con riferimento alle funzioni aziendali di controllo di secondo livello (*risk management* e *compliance*), le banche si conformano entro il 1° luglio 2015 (data di efficacia) a quanto previsto dalla Sezione III, par. 1, lett. *b)*, secondo alinea, secondo periodo («linee di riporto dei responsabili di tali funzioni»);

— con riferimento all'esternalizzazione di funzioni aziendali (Sezioni IV e V), le banche adeguano i contratti di esternalizzazione in essere alla data di entrata in vigore delle presenti disposizioni alla prima scadenza contrattuale e comunque entro tre anni dall'entrata in vigore (1° luglio 2016).

Le banche si conformano alle disposizioni contenute nel Capitolo 8 (*Il sistema informativo*), incluse le raccomandazioni della BCE in materia di sicurezza dei pagamenti in internet, entro il 1° febbraio 2015 (data di efficacia). Le banche adeguano i contratti di esternalizzazione del sistema informativo (Sezione VI) in essere alla data di entrata in vigore delle presenti disposizioni alla prima scadenza contrattuale e comunque entro tre anni dall'entrata in vigore (1° luglio 2016).

Le banche si conformano alle disposizioni contenute nel Capitolo 9 (*La continuità operativa*) entro il 1° luglio 2014 (data di efficacia).

Entro il 31 dicembre 2013 i destinatari della presente disciplina inviano alla Banca d'Italia una relazione recante un'autovalutazione della propria situazione aziendale rispetto alle previsioni della nuova normativa (*gap analysis*). La relazione indica altresì le misure da adottare e la relativa scansione temporale per assicurare il pieno rispetto delle presenti disposizioni. Entro la stessa data, le banche comunicano alla Banca d'Italia i contratti di esternalizzazione in essere alla data di entrata in vigore delle presenti disposizioni e la relativa durata.

Dalla data di efficacia delle norme contenute nei Capitoli 7 (Il sistema dei controlli interni), 8 (Il sistema informativo) e 9 (La continuità operativa) sono abrogate le seguenti disposizioni:

— *Sistema dei controlli interni, compiti del collegio sindacale*, contenute nelle «Istruzioni di vigilanza per le banche», Circolare n. 229 del 21 aprile 1999, Titolo IV, Capitolo 11, ad eccezione della Sezione V (Emissione e gestione di assegni bancari e postali);

— *Continuità operativa in casi di emergenza* (Comunicazione del luglio 2004, *cfr.* Bollettino di vigilanza n. 7 - luglio 2004);

— *La gestione e il controllo dei rischi. Ruolo degli organi aziendali*, contenute nelle «Nuove disposizioni di vigilanza prudenziale per le banche», Circolare n. 263 del 27 dicembre 2006, Titolo I, Capitolo I, Parte Quarta;

— *Disposizioni di vigilanza - Requisiti particolari per la continuità operativa dei processi a rilevanza sistemica* (Comunicazione del marzo 2007, *cfr.* Bollettino di vigilanza n. 3 - marzo 2007);

— *Disposizioni di vigilanza - Esternalizzazione del trattamento del contante* (Comunicazione del 7 maggio 2007), limitatamente agli aspetti concernenti le banche e le capogruppo di gruppi bancari;

— *Disposizioni di vigilanza - la funzione di conformità* (compliance) (Comunicazione del luglio 2007, *cfr.* Bollettino di vigilanza n. 7 - luglio 2007);

— *Comunicazione del 30 dicembre 2008 - Valutazione del merito di credito* (*cfr.* Bollettino di vigilanza n. 12 - dicembre 2008), limitatamente agli aspetti concernenti le banche e le capogruppo di gruppi bancari.

Il testo dell'aggiornamento è disponibile sul sito informatico della Banca d'Italia all'indirizzo:

http://www.bancaditalia.it/vigilanza/banche/normativa/disposizioni/vigprud.

TITOLO V

CAPITOLO 7
IL SISTEMA DEI CONTROLLI INTERNI

Sezione I
DISPOSIZIONI PRELIMINARI E PRINCIPI GENERALI

1. Premessa.

Il sistema dei controlli interni è un elemento fondamentale del complessivo sistema di governo delle banche; esso assicura che l'attività aziendale sia in linea con le strategie e le politiche aziendali e sia improntata a canoni di sana e prudente gestione.

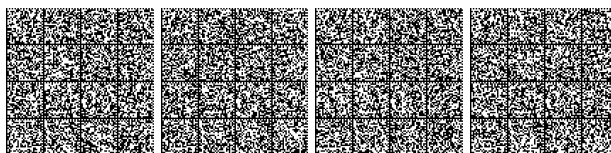
Le presenti disposizioni definiscono i principi e le linee guida cui il sistema dei controlli interni delle banche si deve uniformare; in quest'ambito, sono definiti i principi generali di organizzazione, indicati il ruolo e i compiti degli organi aziendali, delineate le caratteristiche e i compiti delle funzioni aziendali di controllo.

La presente disciplina:

— rappresenta la cornice generale del sistema dei controlli aziendali. In materia di istituti di vigilanza prudenziale, essa è integrata e completata dalle specifiche disposizioni previste in materia (tecniche di attenuazione del rischio di credito ed operazioni di cartolarizzazione, processo ICAAP, informativa al pubblico, concentrazione dei rischi, gestione e controllo del rischio di liquidità, obbligazioni bancarie garantite, partecipazioni detenibili, attività di rischio e conflitti di interesse nei confronti di soggetti collegati, ecc.). Inoltre, alle banche che utilizzano, a fini prudenziali, sistemi interni di misurazione dei rischi diversi da quelli di base o standardizzati, si applicano anche le norme in materia di organizzazione e controlli interni previste dai rispettivi capitoli;

— forma parte integrante del complesso di norme concernenti gli assetti di governo e controllo delle banche, quali le disposizioni di natura organizzativa in materia di: governo societario; *information and communication technology*; assetti proprietari; requisiti degli esponenti aziendali; trasparenza e correttezza delle relazioni tra banche e clienti; attività e servizi di investimento (1); prevenzione dell'utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria a fini di riciclaggio e di finanziamento del terrorismo; usura.

---

(1) Alle banche che prestano attività e servizi di investimento si applicano anche le disposizioni contenute nel Regolamento della Banca d'Italia e della Consob del 29 ottobre 2007, come successivamente modificato e integrato, in materia di organizzazione e procedure degli intermediari che prestano servizi di investimento o di gestione collettiva del risparmio.

I presidi relativi al sistema dei controlli interni devono coprire ogni tipologia di rischio aziendale. La responsabilità primaria è rimessa agli organi aziendali, ciascuno secondo le rispettive competenze. L'articolazione dei compiti e delle responsabilità degli organi e delle funzioni aziendali deve essere chiaramente definita.

Le banche applicano le disposizioni secondo il principio di proporzionalità, cioè tenuto conto della dimensione e complessità operative, della natura dell'attività svolta, della tipologia dei servizi prestati.

La Banca d'Italia, nell'ambito del processo di revisione e valutazione prudenziale, verifica la completezza, la adeguatezza, la funzionalità (in termini di efficienza ed efficacia), la affidabilità del sistema dei controlli interni delle banche.

2. Fonti normative.

La materia è regolata:

— dalla direttiva del Parlamento europeo e del Consiglio 2013/36/UE del 26 giugno 2013, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE;

— dal Regolamento del Parlamento europeo e del Consiglio 2013/575/UE del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento e che modifica il regolamento (UE) n. 648/2012;

— dai seguenti articoli del TUB:

• art. 51, il quale prevede che le banche inviino alla Banca d'Italia, con le modalità e i tempi da essa stabiliti, le segnalazioni periodiche nonché ogni dato e documento richiesti;

• art. 53, comma 1, lett. *d)*, che attribuisce alla Banca d'Italia, in conformità delle delibere del CICR, il potere di emanare disposizioni di carattere generale in materia di organizzazione amministrativa e contabile e controlli interni delle banche;

• art. 67, comma 1, lett. *d)*, che attribuisce alla Banca d'Italia, in conformità delle delibere del CICR, il potere di impartire alla capogruppo di un gruppo bancario disposizioni concernenti il gruppo complessivamente considerato o i suoi componenti aventi ad oggetto l'organizzazione amministrativa e contabile e i controlli interni;

— dalla delibera del CICR del 2 agosto 1996, come modificata dalla delibera del 23 marzo 2004, in materia di organizzazione amministrativa e contabile e controlli interni delle banche e dei gruppi bancari;

— dal decreto del Ministro dell'Economia e delle finanze, Presidente del CICR del 5 agosto 2004 in materia, tra l'altro, di compiti e poteri degli organi sociali delle banche e dei gruppi bancari;

— dalla decisione della BCE del 16 settembre 2010, n. 14, relativa al controllo dell'autenticità e dell'idoneità delle banconote in euro e al loro ricircolo;

Si tiene anche conto dei seguenti documenti pubblicati da istituzioni comunitarie e organismi internazionali: EBA/CEBS: «*Guidelines on the Application of the Supervisory Review Process under Pillar 2*», 25 gennaio 2006; «*Guidelines on outsourcing*», 14 dicembre 2006; «*Guidelines on the management of operational risks in market-related activities*», 12 ottobre 2010; «*Guidelines on Internal Governance*», 27 settembre 2011; Basel Committee on Banking Supervision: «*Fair value measurement and modelling: An assessment of challenges and lessons learned from market stress*», giugno 2008; «*Principle for enhancing corporate governance*», ottobre 2010; «*The internal audit function in banks*», giugno 2012; «*Core Principles for Effective Banking Supervision*», settembre 2012; Financial Stability Board: «*Enhancing Market and Institutional Resilience*», 7 aprile 2008; «*Thematic Review on Risk Governance*», 12 febbraio 2013; European Systemic Risk Board (ESRB): «*Raccomandazione in materia di prestiti in valuta estera (ESRB/2011/1)*», 21 settembre 2011.

3. Definizioni.

Ai fini delle presenti disposizioni si intendono per:

a) «*organo con funzione di supervisione strategica*»: l'organo aziendale a cui — ai sensi del codice civile o per disposizione statutaria — sono attribuite funzioni di indirizzo della gestione dell'impresa, mediante, tra l'altro, esame e delibera in ordine ai piani industriali o finanziari ovvero alle operazioni strategiche;

b) «*organo con funzione di gestione*»: l'organo aziendale o i componenti di esso a cui — ai sensi del codice civile o per disposizione statutaria — spettano o sono delegati compiti di gestione corrente, intesa come attuazione degli indirizzi deliberati nell'esercizio della funzione di supervisione strategica. Il direttore generale rappresenta il vertice della struttura interna e come tale partecipa alla funzione di gestione;

c) «*organo con funzione di controllo*»: il collegio sindacale, il consiglio di sorveglianza o il comitato per il controllo sulla gestione;

d) «*organi aziendali*»: il complesso degli organi con funzioni di supervisione strategica, di gestione e di controllo. La funzione di supervisione strategica e quella di gestione attengono, unitariamente, alla gestione dell'impresa e possono quindi essere incardinate nello stesso organo aziendale. Nei sistemi dualistico e monistico, in conformità delle previsioni legislative, l'organo con funzione di controllo può svolgere anche quella di supervisione strategica;

e) «*funzione aziendale*»: l'insieme dei compiti e delle responsabilità assegnate per l'espletamento di una determinata fase dell'attività aziendale. Sulla base della rilevanza della fase svolta, la funzione è incardinata presso una specifica unità organizzativa;

f) «*funzione antiriciclaggio*»: la funzione definita dal Provvedimento della Banca d'Italia del 10 marzo 2011 recante disposizioni attuative in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria a fini di riciclaggio e di finanziamento del terrorismo, ai sensi dell'art. 7 comma 2 del Decreto Legislativo 21 novembre 2007, n. 231, Capitolo II, Sezione I;

g) «*funzioni aziendali di controllo*»: la funzione di conformità alle norme (*compliance*), la funzione di controllo dei rischi (*risk management function*) e la funzione di revisione interna (*internal audit*) (2);

h) «*funzioni di controllo*»: l'insieme delle funzioni che per disposizione legislativa, regolamentare, statutaria o di autoregolamentazione hanno compiti di controllo;

i) «*funzione operativa importante*»: una funzione operativa per la quale risulta verificata almeno una delle seguenti condizioni:

• un'anomalia nella sua esecuzione o la sua mancata esecuzione possono compromettere gravemente:

a) i risultati finanziari, la solidità o la continuità dell'attività della banca; ovvero

b) la capacità della banca di conformarsi alle condizioni e agli obblighi derivanti dalla sua autorizzazione o agli obblighi previsti dalla disciplina di vigilanza;

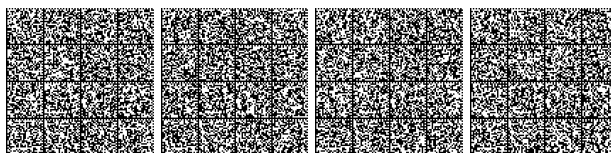
• riguarda attività sottoposte a riserva di legge;

• riguarda processi operativi delle funzioni aziendali di controllo o ha un impatto significativo sulla gestione dei rischi aziendali;

j) «*processo di gestione dei rischi*»: l'insieme delle regole, delle procedure, delle risorse (umane, tecnologiche e organizzative) e delle attività di controllo volte a identificare, misurare o valutare, monitorare, prevenire o attenuare nonché comunicare ai livelli gerarchici appropriati tutti i rischi assunti o assumibili (3) nei diversi segmenti, a livello di portafoglio di impresa e di gruppo, cogliendone, in una logica integrata, anche le interrelazioni reciproche e con l'evoluzione del contesto esterno;

k) «*risk appetite framerwork*» - «RAF» (sistema degli obiettivi di rischio): il quadro di riferimento che definisce — in coerenza con il massimo rischio assumibile, il *business model* e il piano strategico — la propensione al rischio, le soglie di tolleranza, i limiti di rischio, le politiche di governo dei rischi, i processi di riferimento necessari per definirli

(2) Tra le funzioni aziendali di controllo rientrano anche la funzione antiriciclaggio e la funzione di convalida (cfr. Titolo II, Capitolo 1, Parte Seconda, Sezione III, par. 2.1, in materia di Rischio di credito - Metodologia basata sui rating interni (IRB)). Tali funzioni sono disciplinate dalle citate disposizioni e, in quanto compatibile, dal presente Capitolo.

(3) Devono essere considerati, a titolo esemplificativo e non esaustivo, il rischio strategico, il rischio di credito, il rischio di controparte, il rischio di concentrazione, il rischio di mercato, il rischio di tasso di interesse, il rischio operativo, il rischio di liquidità, il rischio di reputazione, il rischio di modello, i rischi derivanti da prestiti in valuta estera, il rischio paese, il rischio di trasferimento nonché i rischi derivanti dall'ambiente macroeconomico in cui la banca opera anche con riferimento all'andamento del ciclo economico. Si riportano, nell'Allegato A, le linee guida riferite a specifiche categorie di rischio, fermo restando quanto previsto nelle specifiche discipline relative alle singole tipologie di rischio.

e attuarli (*cfr.* Allegato C). Si forniscono, di seguito, le definizioni dei concetti rilevanti ai fini del RAF:

• *risk capacity (massimo rischio assumibile)*: il livello massimo di rischio che una banca è tecnicamente in grado di assumere senza violare i requisiti regolamentari o gli altri vincoli imposti dagli azionisti o dall'autorità di vigilanza;

• *risk appetite (obiettivo di rischio o propensione al rischio)*: il livello di rischio (complessivo e per tipologia) che la banca intende assumere per il perseguimento dei suoi obiettivi strategici;

• *risk tolerance (soglia di tollerenza)*: la devianza massima dal *risk appetite* consentita; la soglia di tolleranza è fissata in modo da assicurare in ogni caso alla banca margini sufficienti per operare, anche in condizioni di stress, entro il massimo rischio assumibile. Nel caso in cui sia consentita l'assunzione di rischio oltre l'obiettivo di rischio fissato, fermo restando il rispetto della soglia di tolleranza, sono individuate le azioni gestionali necessarie per ricondurre il rischio assunto entro l'obiettivo prestabilito;

• *risk profile (rischio effettivo)*: il rischio effettivamente assunto, misurato in un determinato istante temporale;

• *risk limits (limiti di rischio)*: l'articolazione degli obiettivi di rischio in limiti operativi, definiti, in linea con il principio di proporzionalità, per tipologie di rischio, unità e o linee di *business*, linee di prodotto, tipologie di clienti;

l) «*esternalizzazione*»: l'accordo in qualsiasi forma tra una banca e un fornitore di servizi in base al quale il fornitore realizza un processo, un servizio o un'attività della stessa banca.

4. Destinatari della disciplina.

Le presenti disposizioni si applicano, secondo quanto stabilito nel Titolo I, Capitolo 1, Parte Seconda:

— alle banche autorizzate in Italia, ad eccezione delle succursali di banche extracomunitarie aventi sede nei paesi del Gruppo dei Dieci o in quelli inclusi in un elenco pubblicato dalla Banca d'Italia (4);

— alle capogruppo di gruppi bancari;

— alle imprese di riferimento, secondo quanto previsto dalla Sezione VI;

— alle succursali di banche comunitarie e alle succursali di banche extracomunitarie aventi sede nei paesi del Gruppo dei Dieci o in quelli inclusi in un elenco pubblicato dalla Banca d'Italia, secondo quanto previsto dalla Sezione VII.

5. Unità organizzative responsabili dei procedimenti amministrativi.

Si indicano di seguito le unità organizzative responsabili dei procedimenti amministrativi di cui al presente Capitolo, ai sensi dell'art. 9 del Regolamento della Banca d'Italia del 25 giugno 2008:

— *divieto dell'esternalizzazione di funzioni operative importanti o di controllo*: Servizio Supervisione gruppi bancari, Servizio Supervisione intermediari specializzati, Filiale competente per territorio;

— *divieto dell'esternalizzazione di funzioni operative importanti o di controllo nell'ambito del gruppo di appartenenza*: Servizio Supervisione gruppi bancari, Servizio Supervisione intermediari specializzati, Filiale competente per territorio.

6. Principi generali.

Il sistema dei controlli interni è costituito dall'insieme delle regole, delle funzioni, delle strutture, delle risorse, dei processi e delle procedure che mirano ad assicurare, nel rispetto della sana e prudente gestione, il conseguimento delle seguenti finalità:

— verifica dell'attuazione delle strategie e delle politiche aziendali;

— contenimento del rischio entro i limiti indicati nel quadro di riferimento per la determinazione della propensione al rischio della banca (*Risk Appetite Framework* - «RAF») (*cfr.* Allegato C);

(4) Alle banche che prestano attività e servizi di investimento si applicano anche le disposizioni contenute nel Regolamento della Banca d'Italia e della Consob del 29 ottobre 2007, come successivamente modificato e integrato, in materia di organizzazione e procedure degli intermediari che prestano servizi di investimento o di gestione collettiva del risparmio.

— salvaguardia del valore delle attività e protezione dalle perdite;

— efficacia ed efficienza dei processi aziendali;

— affidabilità e sicurezza delle informazioni aziendali e delle procedure informatiche (5);

— prevenzione del rischio che la banca sia coinvolta, anche involontariamente, in attività illecite (con particolare riferimento a quelle connesse con il riciclaggio, l'usura ed il finanziamento al terrorismo);

— conformità delle operazioni con la legge e la normativa di vigilanza, nonché con le politiche, i regolamenti e le procedure interne.

Il sistema dei controlli interni riveste un ruolo centrale nell'organizzazione aziendale: rappresenta un elemento fondamentale di conoscenza per gli organi aziendali in modo da garantire piena consapevolezza della situazione ed efficace presidio dei rischi aziendali e delle loro interrelazioni; orienta i mutamenti delle linee strategiche e delle politiche aziendali e consente di adattare in modo coerente il contesto organizzativo; presidia la funzionalità dei sistemi gestionali e il rispetto degli istituti di vigilanza prudenziale; favorisce la diffusione di una corretta cultura dei rischi, della legalità e dei valori aziendali.

Per queste caratteristiche, il sistema dei controlli interni ha rilievo strategico; la cultura del controllo deve avere una posizione di rilievo nella scala dei valori aziendali: non riguarda solo le funzioni aziendali di controllo, ma coinvolge tutta l'organizzazione aziendale (organi aziendali, strutture, livelli gerarchici, personale), nello sviluppo e nell'applicazione di metodi, logici e sistematici, per identificare, misurare, comunicare, gestire i rischi.

Per poter realizzare questo obiettivo, il sistema dei controlli interni deve in generale:

— assicurare la completezza, l'adeguatezza, la funzionalità (in termini di efficienza ed efficacia), l'affidabilità del processo di gestione dei rischi e la sua coerenza con il RAF;

— prevedere attività di controllo diffuse a ogni segmento operativo e livello gerarchico (6);

— garantire che le anomalie riscontrate siano tempestivamente portate a conoscenza di livelli appropriati dell'impresa (agli organi aziendali, se significative) in grado di attivare tempestivamente gli opportuni interventi correttivi;

— incorporare specifiche procedure per far fronte all'eventuale violazione di limiti operativi.

A prescindere dalle strutture dove sono collocate, si possono individuare le seguenti tipologie di controllo:

— *controlli di linea* (c.d. «controlli di primo livello»), diretti ad assicurare il corretto svolgimento delle operazioni. Essi sono effettuati dalle stesse strutture operative (ad es., controlli di tipo gerarchico, sistematici e a campione), anche attraverso unità dedicate esclusivamente a compiti di controllo che riportano ai responsabili delle strutture operative, ovvero eseguiti nell'ambito del *back office*; per quanto possibile, essi sono incorporati nelle procedure informatiche. Le strutture operative sono le prime responsabili del processo di gestione dei rischi: nel corso dell'operatività giornaliera tali strutture devono identificare, misurare o valutare, monitorare, attenuare e riportare i rischi derivanti dall'ordinaria attività aziendale in conformità con il processo di gestione dei rischi; esse devono rispettare i limiti operativi loro assegnati coerentemente con gli obiettivi di rischio e con le procedure in cui si articola il processo di gestione dei rischi;

— *controlli sui rischi e sulla conformità* (c.d. «controlli di secondo livello»), che hanno l'obiettivo di assicurare, tra l'altro:

a) la corretta attuazione del processo di gestione dei rischi;

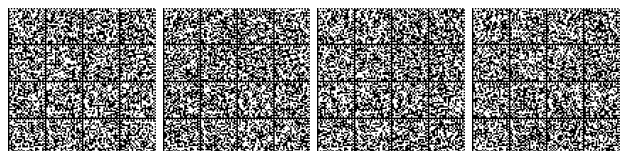
b) il rispetto dei limiti operativi assegnati alle varie funzioni;

c) la conformità dell'operatività aziendale alle norme, incluse quelle di autoregolamentazione.

Le funzioni preposte a tali controlli sono distinte da quelle produttive; esse concorrono alla definizione delle politiche di governo dei rischi e del processo di gestione dei rischi;

— *revisione interna* (c.d. «controlli di terzo livello»), volta a individuare violazioni delle procedure e della regolamentazione nonché a valutare periodicamente la completezza, l'adeguatezza, la funzionalità (in termini di efficienza ed efficacia) e l'affidabilità del sistema dei controlli interni e del sistema informativo (ICT *audit*), con cadenza prefissata in relazione alla natura e all'intensità dei rischi.

(5) Cfr. Capitolo 8 (Il sistema informativo).

(6) Nell'Allegato B sono previsti specifici controlli per le succursali estere di banche italiane.

Presupposto di un sistema dei controlli interni completo e funzionale è l'esistenza di una organizzazione aziendale adeguata per assicurare la sana e prudente gestione delle banche e l'osservanza delle disposizioni loro applicabili.

A tal fine, rileva, in primo luogo, il corretto funzionamento del governo societario, le cui caratteristiche devono essere in linea con quanto previsto nelle disposizioni di vigilanza in materia di organizzazione e governo societario delle banche (7).

Inoltre, le banche rispettano i seguenti principi generali di organizzazione:

— i processi decisionali e l'affidamento di funzioni al personale sono formalizzati e consentono l'univoca individuazione di compiti e responsabilità e sono idonei a prevenire i conflitti di interessi. In tale ambito, deve essere assicurata la necessaria separatezza tra le funzioni operative e quelle di controllo;

— le politiche e le procedure di gestione delle risorse umane assicurano che il personale sia provvisto delle competenze e della professionalità necessarie per l'esercizio delle responsabilità a esso attribuite;

— il processo di gestione dei rischi è efficacemente integrato. Sono considerati parametri di integrazione, riportati a titolo esemplificativo e non esaustivo: la diffusione di un linguaggio comune nella gestione dei rischi a tutti i livelli della banca; l'adozione di metodi e strumenti di rilevazione e valutazione tra di loro coerenti (ad es., un'unica tassonomia dei processi e un'unica mappa dei rischi); la definizione di modelli di reportistica dei rischi, al fine di favorirne la comprensione e la corretta valutazione, anche in una logica integrata; l'individuazione di momenti formalizzati di coordinamento ai fini della pianificazione delle rispettive attività; la previsione di flussi informativi su base continuativa tra le diverse funzioni in relazione ai risultati delle attività di controllo di propria pertinenza; la condivisione nella individuazione delle azioni di rimedio;

— i processi e le metodologie di valutazione, anche a fini contabili, delle attività aziendali sono affidabili e integrati con il processo di gestione del rischio. A tal fine: la definizione e la convalida delle metodologie di valutazione sono affidate a unità differenti; le metodologie di valutazione sono robuste, testate sotto scenari di stress e non fanno affidamento eccessivo su un'unica fonte informativa; la valutazione di uno strumento finanziario è affidata a un'unità indipendente rispetto a quella che negozia detto strumento;

— le procedure operative e di controllo devono: minimizzare i rischi legati a frodi o infedeltà dei dipendenti; prevenire o, laddove non sia possibile, attenuare i potenziali conflitti d'interesse; prevenire il coinvolgimento, anche inconsapevole, in fatti di riciclaggio, usura o di finanziamento al terrorismo;

— il sistema informativo rispetta la disciplina del Capitolo 8 (Il sistema informativo);

— i livelli di continuità operativa garantiti sono adeguati e conformi a quanto stabilito dal Capitolo 9 (La continuità operativa).

Le banche verificano regolarmente, con frequenza almeno annuale, il grado di aderenza ai requisiti del sistema dei controlli interni e dell'organizzazione e adottano le misure adeguate per rimediare a eventuali carenze.

Sezione II IL RUOLO DEGLI ORGANI AZIENDALI

1. Premessa.

Le banche assicurano la completezza, l'adeguatezza, la funzionalità e l'affidabilità del sistema dei controlli interni. In tale ambito, formalizzano il quadro di riferimento per la determinazione della propensione al rischio (*Risk Appetite Framework* - «RAF»), le politiche di governo dei rischi, il processo di gestione dei rischi, ne assicurano l'applicazione e procedono al loro riesame periodico per garantirne l'efficacia nel tempo. La responsabilità primaria è rimessa agli organi aziendali, ciascuno secondo le rispettive competenze.

Nei successivi paragrafi si forniscono indicazioni minime circa il ruolo di ciascun organo aziendale nell'ambito del sistema dei controlli interni, anche al fine di chiarire i relativi compiti e responsabilità.

Tali indicazioni non esauriscono, pertanto, le cautele che possono essere adottate dai competenti organi aziendali nell'ambito della loro autonomia gestionale.

(7) Cfr. «Disposizioni di vigilanza in materia di organizzazione e governo societario delle banche» del 4 marzo 2008 e le relative linee applicative dell'11 gennaio 2012.

2. Organo con funzione di supervisione strategica.

L'organo con funzione di supervisione strategica:

— definisce e approva:

a) il modello di *business* avendo consapevolezza dei rischi cui tale modello espone la banca e comprensione delle modalità attraverso le quali i rischi sono rilevati e valutati;

b) gli indirizzi strategici e provvede al loro riesame periodico, in relazione all'evoluzione dell'attività aziendale e del contesto esterno, al fine di assicurarne l'efficacia nel tempo;

c) gli obiettivi di rischio, la soglia di tolleranza (ove identificata) e le politiche di governo dei rischi;

d) le linee di indirizzo del sistema dei controlli interni, verificando che esso sia coerente con gli indirizzi strategici e la propensione al rischio stabiliti nonché sia in grado di cogliere l'evoluzione dei rischi aziendali e l'interazione tra gli stessi;

e) i criteri per individuare le operazioni di maggiore rilievo da sottoporre al vaglio preventivo della funzione di controllo dei rischi (*cfr.* Sezione III, par. 3.3.);

— approva:

a) la costituzione delle funzioni aziendali di controllo, i relativi compiti e responsabilità, le modalità di coordinamento e collaborazione, i flussi informativi tra tali funzioni e tra queste e gli organi aziendali (*cfr.* anche par. 5);

b) il processo di gestione del rischio e ne valuta la compatibilità con gli indirizzi strategici e le politiche di governo dei rischi;

c) le politiche e i processi di valutazione delle attività aziendali, e, in particolare, degli strumenti finanziari, verificandone la costante adeguatezza; stabilisce altresì i limiti massimi all'esposizione della banca verso strumenti o prodotti finanziari di incerta o difficile valutazione;

d) il processo per lo sviluppo e la convalida dei sistemi interni di misurazione dei rischi non utilizzati a fini regolamentari (8) (9) e ne valuta periodicamente il corretto funzionamento;

e) il processo per l'approvazione di nuovi prodotti e servizi, l'avvio di nuove attività, l'inserimento in nuovi mercati;

f) la politica aziendale in materia di esternalizzazione di funzioni aziendali (*cfr.* Sezioni IV e V);

g) al fine di attenuare i rischi operativi e di reputazione della banca e favorire la diffusione di una cultura dei controlli interni, un codice etico cui sono tenuti a uniformarsi i componenti degli organi aziendali e i dipendenti. Il codice definisce i principi di condotta (ad es., regole deontologiche e regole da osservare nei rapporti con i clienti) a cui deve essere improntata l'attività aziendale;

— assicura che:

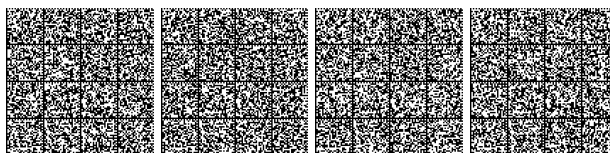
a) la struttura della banca sia coerente con l'attività svolta e con il modello di *business* adottato, evitando la creazione di strutture complesse non giustificate da finalità operative;

b) il sistema dei controlli interni e l'organizzazione aziendale siano costantemente uniformati ai principi indicati nella Sezione I e che le funzioni aziendali di controllo possiedano i requisiti e rispettino le previsioni della Sezione III. Nel caso emergano carenze o anomalie, promuove con tempestività l'adozione di idonee misure correttive e ne valuta l'efficacia;

c) l'attuazione del RAF sia coerente con gli obiettivi di rischio e la soglia di tolleranza (ove identificata) approvati; valuta periodicamente l'adeguatezza e l'efficacia del RAF e la compatibilità tra il rischio effettivo e gli obiettivi di rischio;

d) il piano strategico, il RAF, l'ICAAP, i budget e il sistema dei controlli interni siano coerenti, avuta anche presente l'evoluzione delle condizioni interne ed esterne in cui opera la banca;

(8) Ai fini dell'utilizzo dei sistemi interni di misurazione dei rischi per la determinazione dei requisiti patrimoniali si applicano le specifiche disposizioni organizzative previste nei capitoli che disciplinano le varie tipologie di rischio rilevanti a fini prudenziali.

(9) Per processo di convalida si intende l'insieme formalizzato di attività, strumenti e procedure volti a valutare l'accuratezza delle stime di tutte le componenti rilevanti di rischio e a esprimere un giudizio in merito al regolare funzionamento, alla capacità predittiva e alla performance di un sistema interno di misurazione dei rischi non utilizzato a fini regolamentari.

e) la quantità e l'allocazione del capitale e della liquidità detenuti siano coerenti con la propensione al rischio, le politiche di governo dei rischi e il processo di gestione dei rischi;

— nel caso in cui la banca operi in giurisdizioni poco trasparenti o attraverso strutture particolarmente complesse, valuta i relativi rischi operativi, in particolare di natura legale, reputazionali e finanziari, individua i presidi per attenuarli e ne assicura il controllo effettivo;

— con cadenza almeno annuale, approva il programma di attività, compreso il piano di *audit* predisposto dalla funzione di revisione interna (*cfr.* Sezione III, par. 2), ed esamina le relazioni annuali predisposte dalle funzioni aziendali di controllo. Approva altresì il piano di *audit* pluriennale.

Si indicano, infine, i compiti dell'organo con funzione di supervisione strategica con riguardo a taluni profili specifici:

— con riferimento al processo ICAAP, definisce e approva le linee generali del processo, ne assicura la coerenza con il RAF e l'adeguamento tempestivo in relazione a modifiche significative delle linee strategiche, dell'assetto organizzativo, del contesto operativo di riferimento; promuove il pieno utilizzo delle risultanze dell'ICAAP a fini strategici e nelle decisioni d'impresa;

— riguardo ai rischi di credito e di controparte, approva le linee generali del sistema di gestione delle tecniche di attenuazione del rischio che presiede all'intero processo di acquisizione, valutazione, controllo e realizzo degli strumenti di attenuazione del rischio utilizzati.

Nel caso di banche che adottano sistemi interni di misurazione dei rischi per la determinazione dei requisiti patrimoniali, l'organo con funzione di supervisione strategica svolge anche i seguenti compiti:

— approva l'adozione dei suddetti sistemi. In particolare, approva la scelta del sistema ritenuto idoneo e il relativo progetto in cui sono pianificate le attività connesse con la sua predisposizione e messa in opera, individuate le responsabilità, definiti i tempi di realizzazione, determinati gli investimenti previsti in termini di risorse umane, finanziarie e tecnologiche;

— verifica periodicamente che le scelte effettuate mantengano nel tempo la loro validità, approvando i cambiamenti sostanziali al sistema e provvedendo alla complessiva supervisione sul corretto funzionamento dello stesso;

— vigila, con il supporto delle competenti funzioni, sull'effettivo utilizzo dei sistemi interni a fini gestionali (*use test*) e sulla loro rispondenza agli altri requisiti previsti dalla normativa;

— con cadenza almeno annuale, esamina i riferimenti forniti dalla funzione di convalida e assume, col parere dell'organo con funzione di controllo, formale delibera con la quale attesta il rispetto dei requisiti previsti per l'utilizzo dei sistemi.

3. Organo con funzione di gestione.

L'organo con funzione di gestione ha la comprensione di tutti i rischi aziendali, inclusi i possibili rischi di malfunzionamento dei sistemi interni di misurazione (c.d. «rischio di modello»), e, nell'ambito di una gestione integrata, delle loro interrelazioni reciproche e con l'evoluzione del contesto esterno. In tale ambito, è in grado di individuare e valutare i fattori, inclusa la complessità della struttura organizzativa, da cui possono scaturire rischi per la banca.

Tale organo cura l'attuazione degli indirizzi strategici, del RAF e delle politiche di governo dei rischi definiti dall'organo con funzione di supervisione strategica ed è responsabile per l'adozione di tutti gli interventi necessari ad assicurare l'aderenza dell'organizzazione e del sistema dei controlli interni ai principi e requisiti di cui alle Sezioni I e III, monitorandone nel continuo il rispetto.

In particolare, l'organo con funzione di gestione:

— definisce e cura l'attuazione del processo di gestione dei rischi. In tale ambito:

a) stabilisce limiti operativi all'assunzione delle varie tipologie di rischio, coerenti con la propensione al rischio, tenendo esplicitamente conto dei risultati delle prove di stress e dell'evoluzione del quadro economico. Inoltre, nell'ambito della gestione dei rischi, limita l'affidamento sui *rating* esterni, assicurando che, per ciascuna tipologia di rischio, siano condotte adeguate e autonome analisi interne;

b) agevola lo sviluppo e la diffusione a tutti i livelli di una cultura del rischio integrata in relazione alle diverse tipologie di rischi ed estesa a tutta la banca. In particolare, sono sviluppati e attuati programmi di formazione per sensibilizzare i dipendenti in merito alle responsabilità in materia di rischi in modo da non confinare il processo di gestione del rischio agli specialisti o alle funzioni di controllo;

c) stabilisce le responsabilità delle strutture e delle funzioni aziendali coinvolte nel processo di gestione dei rischi, in modo che siano chiaramente attribuiti i relativi compiti e siano prevenuti potenziali conflitti d'interessi; assicura, altresì, che le attività rilevanti siano dirette da personale qualificato, con adeguato grado di autonomia di giudizio e in possesso di esperienze e conoscenze adeguate ai compiti da svolgere;

d) esamina le operazioni di maggior rilievo oggetto di parere negativo da parte della funzione di controllo dei rischi e, se del caso, le autorizza (*cfr.* Sezione III, par. 3.3.); di tali operazioni informa l'organo con funzione di supervisione strategica e l'organo con funzione di controllo;

— definisce e cura l'attuazione del processo (responsabili, procedure, condizioni) per approvare gli investimenti in nuovi prodotti, la distribuzione di nuovi prodotti o servizi ovvero l'avvio di nuove attività o l'ingresso in nuovi mercati. Il processo:

a) assicura che vengano pienamente valutati i rischi derivanti dalla nuova operatività, che detti rischi siano coerenti con la propensione al rischio e che la banca sia in grado di gestirli;

b) definisce le fasce di clientela a cui si intendono distribuire nuovi prodotti o servizi in relazione alla complessità degli stessi e a eventuali vincoli normativi esistenti;

c) consente di stimare gli impatti della nuova operatività in termini di costi, ricavi, risorse (umane, organizzative e tecnologiche) nonché di valutare gli impatti sulle procedure amministrative e contabili della banca;

d) individua le eventuali modifiche da apportare al sistema dei controlli interni;

— definisce e cura l'attuazione della politica aziendale in materia di esternalizzazione di funzioni aziendali (*cfr.* Sezioni IV e V);

— definisce e cura l'attuazione dei processi e delle metodologie di valutazione delle attività aziendali, e, in particolare, degli strumenti finanziari; ne cura il loro costante aggiornamento;

— definisce i flussi informativi interni volti ad assicurare agli organi aziendali e alle funzioni aziendali di controllo la piena conoscenza e governabilità dei fattori di rischio e la verifica del rispetto del RAF;

— nell'ambito del RAF, se è stata definita la soglia di tolleranza, autorizza il superamento della propensione al rischio entro il limite rappresentato dalla soglia di tolleranza e provvede a darne pronta informativa all'organo con funzione di supervisione strategica, individuando le azioni gestionali necessarie per ricondurre il rischio assunto entro l'obiettivo prestabilito;

— pone in essere le iniziative e gli interventi necessari per garantire nel continuo la completezza, l'adeguatezza, la funzionalità e l'affidabilità del sistema dei controlli interni e porta i risultati delle verifiche effettuate a conoscenza dell'organo con funzione di supervisione strategica;

— predispone e attua i necessari interventi correttivi o di adeguamento nel caso emergano carenze o anomalie, o a seguito dell'introduzione di nuovi prodotti, attività, servizi o processi rilevanti;

— assicura:

a) la coerenza del processo di gestione dei rischi con la propensione al rischio e le politiche di governo dei rischi, avuta anche presente l'evoluzione delle condizioni interne ed esterne in cui opera la banca;

b) una corretta, tempestiva e sicura gestione delle informazioni a fini contabili, gestionali e di *reporting*.

Si indicano, infine, i compiti dell'organo con funzione di gestione con riguardo a taluni profili specifici:

— con riferimento al processo ICAAP, dà attuazione a tale processo curando che lo stesso sia rispondente agli indirizzi strategici e la RAF e che soddisfi i seguenti requisiti: consideri tutti i rischi rilevanti; incorpori valutazioni prospettiche; utilizzi appropriate metodologie; sia conosciuto e condiviso dalle strutture interne; sia adeguatamente formalizzato e documentato; individui i ruoli e le responsabilità assegnate alle funzioni e alle strutture aziendali; sia affidato a risorse competenti, sufficienti sotto il profilo quantitativo, collocate in posizione gerarchica adeguata a far rispettare la pianificazione; sia parte integrante dell'attività gestionale;

— con specifico riferimento ai rischi di credito e di controparte, in linea con gli indirizzi strategici, approva specifiche linee guida volte ad assicurare l'efficacia del sistema di gestione delle tecniche di attenuazione del rischio e a garantire il rispetto dei requisiti generali e specifici di tali tecniche.

Nel caso di banche che adottano sistemi interni di misurazione dei rischi per la determinazione dei requisiti patrimoniali, l'organo con funzione di gestione svolge anche i seguenti compiti:

— è responsabile dell'impianto e del funzionamento del sistema prescelto; per svolgere tale compito i componenti dell'organo possiedono un'adeguata conoscenza degli aspetti rilevanti;

— impartisce le disposizioni necessarie affinché il sistema prescelto sia realizzato secondo le linee strategiche individuate, assegnando compiti e responsabilità alle diverse funzioni aziendali e assicurando la formalizzazione e la documentazione delle fasi del processo di gestione del rischio;

— cura che i sistemi di misurazione dei rischi siano integrati nei processi decisionali e nella gestione dell'operatività aziendale (*use test*);

— tiene conto, nello svolgimento dei compiti assegnati, delle osservazioni emerse a seguito del processo di convalida e delle verifiche condotte dalla revisione interna.

4. Organo con funzione di controllo.

L'organo con funzione di controllo ha la responsabilità di vigilare sulla completezza, adeguatezza, funzionalità e affidabilità del sistema dei controlli interni e del RAF.

Nell'espletamento di tale compito, l'organo con funzione di controllo vigila sul rispetto delle previsioni di cui *i)* alla presente Sezione, *ii)* alle Sezioni I e III e *iii)* al processo ICAAP. Per lo svolgimento delle proprie attribuzioni, tale organo dispone di adeguati flussi informativi da parte degli altri organi aziendali e delle funzioni di controllo.

L'organo con funzione di controllo svolge, di norma, le funzioni dell'organismo di vigilanza — eventualmente istituito ai sensi del d.lgs. n. 231/2001, in materia di responsabilità amministrativa degli enti — che vigila sul funzionamento e l'osservanza dei modelli di organizzazione e di gestione di cui si dota la banca per prevenire i reati rilevanti ai fini del medesimo decreto legislativo (10). Le banche possono affidare tali funzioni a un organismo appositamente istituito dandone adeguata motivazione.

Considerata la pluralità di funzioni aventi, all'interno dell'azienda, compiti e responsabilità di controllo, l'organo con funzione di controllo è tenuto ad accertare l'adeguatezza di tutte le funzioni coinvolte nel sistema dei controlli, il corretto assolvimento dei compiti e l'adeguato coordinamento delle medesime, promuovendo gli interventi correttivi delle carenze e delle irregolarità rilevate (11).

Nelle banche che adottano sistemi interni di misurazione dei rischi per la determinazione dei requisiti patrimoniali, l'organo con funzione di controllo, avvalendosi dell'apporto delle funzioni aziendali di controllo, vigila — nell'ambito della più generale attività di verifica del processo di gestione dei rischi — sulla completezza, adeguatezza, funzionalità, affidabilità, dei sistemi stessi e sulla loro rispondenza ai requisiti previsti dalla normativa.

5. Il coordinamento delle funzioni di controllo.

Il corretto funzionamento del sistema dei controlli interni si basa sulla proficua interazione nell'esercizio dei compiti (d'indirizzo, di attuazione, di verifica, di valutazione) fra gli organi aziendali, gli eventuali comitati costituiti all'interno di questi ultimi (12), i soggetti incaricati della revisione legale dei conti, le funzioni di controllo.

L'ordinamento e le fonti di autoregolamentazione attribuiscono, poi, compiti di controllo a specifiche funzioni — diverse dalle funzioni aziendali di controllo — o a comitati interni all'organo amministrativo, la cui attività va inquadrata in modo coerente nel sistema dei controlli interni.

In particolare, rilevano:

— l'organismo di vigilanza eventualmente istituito ai sensi del d.lgs. n. 231/2001;

— per le banche con azioni quotate, il dirigente preposto alla redazione dei documenti contabili societari (art. 154-*bis* del TUF), il quale, tra l'altro, ha il compito di stabilire adeguate procedure amministrative e contabili per la predisposizione del bilancio e di ogni altra comunicazione di carattere finanziario.

Inoltre, il Codice di autodisciplina della Borsa Italiana, a cui le banche quotate possono aderire su base volontaria, introduce principi e criteri applicativi riguardo al sistema di controllo interno e di gestione dei rischi, che prevedono, tra l'altro, la designazione di uno o più amministratori incaricati del sistema di controllo interno e di gestione dei rischi e l'istituzione, in seno all'organo amministrativo, di un comitato controllo e rischi.

Per assicurare una corretta interazione tra tutte le funzioni e organi con compiti di controllo, evitando sovrapposizioni o lacune, l'organo con funzione di supervisione strategica approva un documento, diffuso a tutte le strutture interessate, nel quale sono definiti i compiti e le responsabilità dei vari organi e funzioni di controllo, i flussi informativi tra le diverse funzioni/organi e tra queste/i e gli organi aziendali e, nel caso in cui gli ambiti di controllo presentino aree di potenziale sovrapposizione o permettano di sviluppare sinergie, le modalità di coordinamento e di collaborazione. A titolo esemplificativo, nell'attività dell'organismo di vigilanza, che attiene in generale all'adempimento di leggi e regolamenti, può essere proficuo uno stretto raccordo, in termini sia di suddivisione di attività che di condivisione di informazioni, con le funzioni di conformità alle norme e di revisione interna.

Nel definire le modalità di raccordo, ferme restando le attribuzioni previste dalla legge per le funzioni di controllo, le banche prestano attenzione a non alterare, anche nella sostanza, le responsabilità primarie degli organi aziendali sul sistema dei controlli interni.

Sezione III
FUNZIONI AZIENDALI DI CONTROLLO

1. Istituzione delle funzioni aziendali di controllo.

Ferma restando l'autonoma responsabilità aziendale per le scelte effettuate in materia di assetto dei controlli interni, le banche istituiscono, secondo quanto di seguito indicato, funzioni aziendali di controllo permanenti e indipendenti: *i)* di conformità alle norme (*compliance*); *ii)* di controllo dei rischi (*risk management*); *iii)* di revisione interna (*internal audit*).

Le prime due funzioni attengono ai controlli di secondo livello, la revisione interna ai controlli di terzo livello.

Per assicurare l'indipendenza delle funzioni aziendali di controllo:

a) tali funzioni dispongono dell'autorità, delle risorse e delle competenze necessarie per lo svolgimento dei loro compiti. Alle funzioni è consentito di avere accesso ai dati aziendali e a quelli esterni necessari per svolgere in modo appropriato i propri compiti. Le risorse economiche, eventualmente attivabili in autonomia, permettono, tra l'altro, alle funzioni aziendali di controllo di ricorrere a consulenze esterne. Il personale è adeguato per numero, competenze tecnico-professionali, aggiornamento, anche attraverso l'inserimento di programmi di formazione nel continuo. Al fine di garantire la formazione di competenze trasversali e di acquisire una visione complessiva e integrata dell'attività di controllo svolta dalla funzione, la banca formalizza e incentiva programmi di rotazione delle risorse, tra le funzioni aziendali di controllo;

b) i responsabili:

• possiedono requisiti di professionalità adeguati;

• sono collocati in posizione gerarchico-funzionale adeguata. In particolare, i responsabili delle funzioni di controllo dei rischi e di conformità alle norme sono collocati alle dirette dipendenze dell'organo con funzione di gestione o dell'organo con funzione di supervisione strategica; il responsabile della funzione di revisione interna è collocato sempre alle dirette dipendenze dell'organo con funzione di supervisione strategica;

• non hanno responsabilità diretta di aree operative sottoposte a controllo né sono gerarchicamente subordinati ai responsabili di tali aree;

---

(10) In particolare, i citati modelli organizzativi e di gestione sono volti a: i) individuare le attività nel cui ambito possono essere commessi reati; ii) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire; iii) individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati; iv) prevedere obblighi di informazione nei confronti dell'organismo di vigilanza; v) definire un sistema sanzionatorio per il mancato rispetto delle misure indicate nel citato modello.

(11) Cfr. «Disposizioni di vigilanza in materia di organizzazione e governo societario delle banche» del 4 marzo 2008 e le relative linee applicative dell'11 gennaio 2012, cui si rimanda per la descrizione dettagliata dei compiti e poteri dell'organo con funzione di controllo.

(12) Cfr. «Disposizioni di vigilanza in materia di organizzazione e governo societario delle banche» del 4 marzo 2008 e le relativa linee applicative dell'11 gennaio 2012, cui si rimanda per la descrizione dettagliata dei compiti e poteri dell'organo con funzione di controllo.

• sono nominati e revocati (motivandone le ragioni) dall'organo con funzione di supervisione strategica, sentito l'organo con funzione di controllo (13). Il responsabile di funzioni aziendali di controllo può essere un componente dell'organo amministrativo, purché sia destinatario di specifiche deleghe in materia di controlli e non sia destinatario di altre deleghe che ne pregiudichino l'autonomia;

• riferiscono direttamente agli organi aziendali. In particolare, i responsabili della funzione di controllo dei rischi e della funzione di conformità alle norme hanno, in ogni caso, accesso diretto all'organo con funzione di supervisione strategica e all'organo con funzione di controllo e comunicano con essi senza restrizioni o intermediazioni; il responsabile della funzione di revisione interna ha accesso diretto all'organo con funzione di controllo e comunica con esso senza restrizioni o intermediazioni;

c) il personale che partecipa alle funzioni aziendali di controllo non è coinvolto in attività che tali funzioni sono chiamate a controllare. Nel rispetto di tale principio, nelle banche di dimensioni contenute o caratterizzate da una limitata complessità operativa, il personale incaricato di compiti attinenti al controllo di conformità alle norme o al controllo dei rischi, qualora non sia inserito nelle relative funzioni aziendali di controllo, può essere integrato in aree operative diverse; in questi casi, tale personale riferisce direttamente ai responsabili delle funzioni aziendali di controllo per le questioni attinenti ai compiti di tali funzioni;

d) le funzioni aziendali di controllo sono tra loro separate, sotto un profilo organizzativo. I rispettivi ruoli e responsabilità sono formalizzati;

e) i criteri di remunerazione del personale che partecipa alle funzioni aziendali di controllo non ne compromettono l'obiettività e concorrono a creare un sistema di incentivi coerente con le finalità della funzione svolta (14).

Se coerente con il principio di proporzionalità, le banche possono, a condizione che i controlli sulle diverse tipologie di rischio continuino ad essere efficaci:

— affidare a un'unica struttura lo svolgimento della funzione di conformità alle norme e della funzione di controllo dei rischi;

— affidare lo svolgimento delle funzioni aziendali di controllo all'esterno, secondo quanto previsto dalle disposizioni in materia di esternalizzazione previste nella Sezione IV e, per quanto riguarda l'esternalizzazione all'interno dei gruppi bancari, nella Sezione V.

Tenuto conto che le funzioni di conformità alle norme e di controllo dei rischi devono essere sottoposte a verifica periodica da parte della funzione di revisione interna (controllo di terzo livello), per assicurare l'imparzialità delle verifiche, le funzioni di conformità alle norme e di gestione dei rischi non possono essere affidate alla funzione di revisione interna.

2. Programmazione e rendicontazione dell'attività di controllo.

Per ciascuna funzione aziendale di controllo, la regolamentazione interna indica responsabilità, compiti, modalità operative, flussi informativi, programmazione dell'attività di controllo.

In particolare:

— le funzioni di conformità alle norme e di controllo dei rischi presentano annualmente agli organi aziendali, ciascuna in base alle rispettive competenze, un programma di attività, in cui sono identificati e valutati i principali rischi a cui la banca è esposta e sono programmati i relativi interventi di gestione. La programmazione degli interventi tiene conto sia delle eventuali carenze emerse nei controlli, sia di eventuali nuovi rischi identificati;

— la funzione di revisione interna presenta annualmente agli organi aziendali un piano di *audit*, che indica le attività di controllo pianificate, tenuto conto dei rischi delle varie attività e strutture aziendali; il piano contiene una specifica sezione relativa all'attività di revisione del sistema informativo (ICT *auditing*).

Al termine del ciclo gestionale, con cadenza quindi annuale, le funzioni aziendali di controllo:

— presentano agli organi aziendali una relazione dell'attività svolta, che illustra le verifiche effettuate, i risultati emersi, i punti di debolezza rilevati e propongono gli interventi da adottare per la loro rimozione;

— riferiscono, ciascuna per gli aspetti di rispettiva competenza, in ordine alla completezza, adeguatezza, funzionalità e affidabilità del sistema dei controlli interni.

In ogni caso, le funzioni aziendali di controllo informano tempestivamente gli organi aziendali su ogni violazione o carenza rilevante riscontrate (ad es., violazioni che possono comportare un alto rischio di sanzioni regolamentari o legali, perdite finanziarie di rilievo o significativi impatti sulla situazione finanziaria o patrimoniale, danni di reputazione, malfunzionamenti di procedure informatiche critiche).

3. Requisiti specifici delle funzioni aziendali di controllo.

3.1. *Premessa*.

Nei paragrafi seguenti si stabiliscono, in via generale, le responsabilità e i principali compiti di ciascuna delle funzioni aziendali di controllo (15).

Indicazioni più specifiche concernenti le responsabilità e i compiti di tali funzioni relativamente a ciascuna singola categoria di rischio, ambiti operativi o attività particolari sono riportate nelle relative discipline (*cfr.* Sezione I, par. 1).

3.2. *Funzione di conformità alle norme (*compliance*)*.

Il rischio di non conformità alle norme è il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di violazioni di norme imperative (leggi, regolamenti) ovvero di autoregolamentazione (ad es., statuti, codici di condotta, codici di autodisciplina).

Poiché il rischio di non conformità alle norme è diffuso a tutti livelli dell'organizzazione aziendale, soprattutto nell'ambito delle linee operative, l'attività di prevenzione deve svolgersi in primo luogo dove il rischio viene generato: è pertanto necessaria un'adeguata responsabilizzazione di tutto il personale.

La funzione di conformità alle norme presiede, secondo un approccio *risk based*, alla gestione del rischio di non conformità con riguardo a tutta l'attività aziendale, verificando che le procedure interne siano adeguate a prevenire tale rischio. A tal fine, è necessario che la funzione di conformità alle norme abbia accesso a tutte le attività della banca, centrali e periferiche, e a qualsiasi informazione a tal fine rilevante, anche attraverso il colloquio diretto con il personale.

I principali adempimenti che la funzione di conformità alle norme è chiamata a svolgere sono:

— l'ausilio alle strutture aziendali per la definizione delle metodologie di valutazione dei rischi di non conformità alle norme;

— l'individuazione di idonee procedure per la prevenzione del rischio rilevato, con possibilità di richiederne l'adozione; la verifica della loro adeguatezza e corretta applicazione;

— l'identificazione nel continuo delle norme applicabili alla banca e la misurazione/valutazione del loro impatto su processi e procedure aziendali;

— la proposta di modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio dei rischi di non conformità identificati;

— la predisposizione di flussi informativi diretti agli organi aziendali e alle strutture coinvolte (ad es.: gestione del rischio operativo e revisione interna);

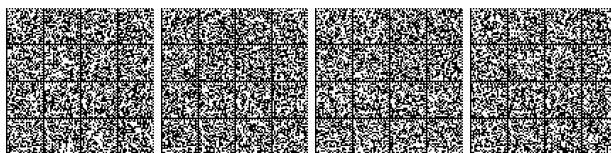
— la verifica dell'efficacia degli adeguamenti organizzativi (strutture, processi, procedure anche operative e commerciali) suggeriti per la prevenzione del rischio di non conformità alle norme.

Per le norme più rilevanti ai fini del rischio di non conformità, quali quelle che riguardano l'esercizio dell'attività bancaria e di intermediazione, la gestione dei conflitti di interesse, la trasparenza nei confronti della clientela e, più in generale, la disciplina posta a tutela del consumatore, e per quelle norme per le quali non siano già previste forme di presidio specializzato all'interno della banca, la funzione è direttamente responsabile della gestione del rischio di non conformità.

Con riferimento ad altre normative per le quali siano già previste forme specifiche di presidio specializzato (ad es.: normativa sulla sicurezza sul lavoro, in materia di trattamento dei dati personali), la banca,

(13) I responsabili delle funzioni aziendali di controllo sono nominati secondo procedure di selezione formalizzate.

(14) Cfr. «Disposizioni in materia di politiche e prassi di remunerazione e incentivazione nelle banche e nei gruppi bancari» del 30 marzo 2011.

(15) Con esclusivo riferimento alla prestazione di attività e servizi di investimento, si applica il riparto di competenze tra la funzione di conformità alle norme e la funzione di revisione interna previsto dalla Comunicazione congiunta Banca d'Italia - Consob dell'8 marzo 2011.

in base a una valutazione dell'adeguatezza dei controlli specialistici a gestire i profili di rischio di non conformità, può graduare i compiti della *compliance*, che comunque è responsabile, in collaborazione con le funzioni specialistiche incaricate, almeno della definizione delle metodologie di valutazione del rischio di non conformità e della individuazione delle relative procedure, e procede alla verifica dell'adeguatezza delle procedure medesime a prevenire il rischio di non conformità.

La banca può adottare tale approccio anche con riferimento al presidio del rischio di non conformità alle normative di natura fiscale (16), che richiede almeno: *(i)* la definizione di procedure (17) volte a prevenire violazioni o elusioni di tale normativa e ad attenuare i rischi connessi a situazioni che potrebbero integrare fattispecie di abuso del diritto, in modo da minimizzare le conseguenze sia sanzionatorie, sia reputazionali derivanti dalla non corretta applicazione della normativa fiscale; *(ii)* la verifica dell'adeguatezza di tali procedure e della loro idoneità a realizzare effettivamente l'obiettivo di prevenire il rischio di non conformità.

Ferme restando le responsabilità della funzione di *compliance* per l'espletamento dei compiti previsti da normative specifiche (quali, ad es., le discipline in materia di politiche e prassi di remunerazione e incentivazione, di trasparenza delle operazioni e correttezza delle relazioni tra intermediari e clienti e di attività di rischio e conflitti di interesse nei confronti di soggetti collegati), altre aree di intervento sono:

— il coinvolgimento nella valutazione *ex ante* della conformità alla regolamentazione applicabile di tutti i progetti innovativi (inclusa l'operatività in nuovi prodotti o servizi) che la banca intenda intraprendere nonché nella prevenzione e nella gestione dei conflitti di interesse sia tra le diverse attività svolte dalla banca, sia con riferimento ai dipendenti e agli esponenti aziendali;

— la consulenza e assistenza nei confronti degli organi aziendali della banca in tutte le materie in cui assume rilievo il rischio di non conformità nonché la collaborazione nell'attività di formazione del personale sulle disposizioni applicabili alle attività svolte, al fine di diffondere una cultura aziendale improntata ai principi di onestà, correttezza e rispetto dello spirito e della lettera delle norme.

Sotto il profilo organizzativo, tenuto conto dei molteplici profili professionali richiesti per l'espletamento di tali adempimenti, le varie fasi in cui si articola l'attività della funzione di conformità alle norme possono essere affidate a risorse appartenenti ad altre strutture organizzative (ad es., legale, organizzazione, gestione del rischio operativo), purché il processo di gestione del rischio e l'operatività della funzione siano ricondotti ad unità mediante la nomina di un responsabile che coordini e sovrintenda alle diverse attività.

3.3. *Funzione di controllo dei rischi (*risk management function*).*

La funzione di controllo dei rischi ha la finalità di collaborare alla definizione e all'attuazione del RAF e delle relative politiche di governo dei rischi, attraverso un adeguato processo di gestione dei rischi (18).

La funzione di controllo dei rischi deve essere organizzata in modo da perseguire in maniera efficiente ed efficace tale obiettivo. Essa può essere variamente articolata, ad esempio in relazione ai singoli profili di rischio (di credito, di mercato, operativo, modello, ecc.), purché la banca mantenga una visione d'insieme dei diversi rischi e della loro reciproca interazione. Le banche che adottano sistemi interni per la misurazione dei rischi, se coerente con la natura, la dimensione e la complessità dell'attività svolta, individuano all'interno della funzione di controllo dei rischi unità preposte alla convalida di detti sistemi indipendenti dalle unità responsabili dello sviluppo degli stessi.

Specie nelle banche più complesse, può essere prevista la costituzione di specifici comitati di gestione dei diversi profili di rischio (ad es., comitati per i rischi di credito e operativi, comitato di liquidità, comitato finanza, comitato per l'*asset and liability management*), definendo in modo chiaro le diverse responsabilità e le modalità di intervento e di partecipazione della funzione, in modo da garantirne la completa indipendenza dal processo di assunzione dei rischi; va inoltre evitato che l'istituzione di tali comitati possa depotenziare le prerogative della funzione di controllo dei rischi.

Al tempo stesso, vanno individuate soluzioni organizzative che non determinino una eccessiva distanza dal contesto operativo. Per la piena consapevolezza dei rischi è necessario che vi sia una continua interazione critica con le unità di *business*.

La funzione di controllo dei rischi:

— è coinvolta nella definizione del RAF, delle politiche di governo dei rischi e delle varie fasi che costituiscono il processo di gestione dei rischi nonché nella fissazione dei limiti operativi all'assunzione delle varie tipologie di rischio. In tale ambito, ha, tra l'altro, il compito di proporre i parametri quantitativi e qualitativi necessari per la definizione del RAF, che fanno riferimento anche a scenari di stress e, in caso di modifiche del contesto operativo interno ed esterno della banca, l'adeguamento di tali parametri;

— verifica l'adeguatezza del RAF;

— verifica nel continuo l'adeguatezza del processo di gestione dei rischi e dei limiti operativi;

— fermo restando quanto previsto nell'ambito della disciplina dei sistemi interni per il calcolo dei requisiti patrimoniali, è responsabile dello sviluppo, della convalida e del mantenimento dei sistemi di misurazione e controllo dei rischi assicurando che siano sottoposti a *backtesting* periodici, che vengano analizzati un appropriato numero di scenari e che siano utilizzate ipotesi conservative sulle dipendenze e sulle correlazioni; nella misurazione dei rischi tiene conto in generale del rischio di modello e dell'eventuale incertezza nella valutazione di alcune tipologie di strumenti finanziari e informa di queste incertezze l'organo con funzione di gestione;

— definisce metriche comuni di valutazione dei rischi operativi coerenti con il RAF, coordinandosi con la funzione di conformità alle norme, con la funzione ICT e con la funzione di continuità operativa;

— definisce modalità di valutazione e controllo dei rischi reputazionali, coordinandosi con la funzione di conformità alle norme e le funzioni aziendali maggiormente esposte;

— coadiuva gli organi aziendali nella valutazione del rischio strategico monitorando le variabili significative;

— assicura la coerenza dei sistemi di misurazione e controllo dei rischi con i processi e le metodologie di valutazione delle attività aziendali, coordinandosi con le strutture aziendali interessate;

— sviluppa e applica indicatori in grado di evidenziare situazioni di anomalia e di inefficienza dei sistemi di misurazione e controllo dei rischi;

— analizza i rischi dei nuovi i prodotti e servizi e di quelli derivanti dall'ingresso in nuovi segmenti operativi e di mercato;

— dà pareri preventivi sulla coerenza con il RAF delle operazioni di maggiore rilievo eventualmente acquisendo, in funzione della natura dell'operazione, il parere di altre funzioni coinvolte nel processo di gestione dei rischi;

— monitora costantemente il rischio effettivo assunto dalla banca e la sua coerenza con gli obiettivi di rischio nonché il rispetto dei limiti operativi assegnati alle strutture operative in relazione all'assunzione delle varie tipologie di rischio;

— verifica il corretto svolgimento del monitoraggio andamentale sulle singole esposizioni creditizie (*cfr.* Allegato A, par. 2);

— verifica l'adeguatezza e l'efficacia delle misure prese per rimediare alle carenze riscontrate nel processo di gestione del rischio.

3.4. *Funzione di revisione interna (*internal audit*).*

La funzione di revisione interna è volta, da un lato, a controllare, in un'ottica di controlli di terzo livello, anche con verifiche in loco, il regolare andamento dell'operatività e l'evoluzione dei rischi, e, dall'altro, a valutare la completezza, l'adeguatezza, la funzionalità e l'affidabilità della struttura organizzativa e delle altre componenti del sistema dei controlli interni, portando all'attenzione degli organi aziendali i possibili miglioramenti, con particolare riferimento al RAF, al processo di gestione dei rischi nonché agli strumenti di misurazione e controllo degli stessi. Sulla base dei risultati dei propri controlli formula raccomandazioni agli organi aziendali.

(16) Le banche devono altresì tener conto dei rischi derivanti dal coinvolgimento in operazioni fiscalmente irregolari poste in essere dalla clientela.

(17) Tali procedure possono prevedere il ricorso a figure interne alla banca esperte in materia fiscale oppure, nei casi più complessi, l'acquisizione del parere delle autorità tributarie competenti.

(18) La funzione di controllo dei rischi va tenuta distinta e indipendente dalle funzioni aziendali incaricate della «gestione operativa» dei rischi, che incidono sull'assunzione dei rischi da parte delle unità di business e modificano il profilo di rischio della banca.

In tale ambito, coerentemente con il piano di *audit*, la funzione di revisione interna:

— valuta la completezza, l'adeguatezza, la funzionalità, l'affidabilità delle altre componenti del sistema dei controlli interni, del processo di gestione dei rischi e degli altri processi aziendali, avendo riguardo anche alla capacità di individuare errori ed irregolarità. In tale contesto, sottopone, tra l'altro, a verifica le funzioni aziendali di controllo dei rischi e di conformità alle norme;

— valuta l'efficacia del processo di definizione del RAF, la coerenza interna dello schema complessivo e la conformità dell'operatività aziendale al RAF e, in caso di strutture finanziarie particolarmente complesse, la conformità di queste alle strategie approvate dagli organi aziendali;

— verifica, anche attraverso accertamenti di natura ispettiva:

a) la regolarità delle diverse attività aziendali, incluse quelle esternalizzate, e l'evoluzione dei rischi sia nella direzione generale della banca, sia nelle filiali. La frequenza delle ispezioni è coerente con l'attività svolta e la propensione al rischio; tuttavia sono condotti anche accertamenti ispettivi casuali e non preannunciati;

b) il monitoraggio della conformità alle norme dell'attività di tutti i livelli aziendali;

c) il rispetto, nei diversi settori operativi, dei limiti previsti dai meccanismi di delega, e il pieno e corretto utilizzo delle informazioni disponibili nelle diverse attività;

d) l'efficacia dei poteri della funzione di controllo dei rischi di fornire pareri preventivi sulla coerenza con il RAF delle operazioni di maggior rilievo;

e) l'adeguatezza e il corretto funzionamento dei processi e delle metodologie di valutazione delle attività aziendali e, in particolare, degli strumenti finanziari;

f) l'adeguatezza, l'affidabilità complessiva e la sicurezza del sistema informativo (ICT *audit*);

g) la rimozione delle anomalie riscontrate nell'operatività e nel funzionamento dei controlli (attività di «*follow-up*»);

— effettua test periodici sul funzionamento delle procedure operative e di controllo interno;

— espleta compiti d'accertamento anche con riguardo a specifiche irregolarità;

— controlla regolarmente il piano aziendale di continuità operativa. In tale ambito, prende visione dei programmi di verifica, assiste alle prove e ne controlla i risultati, propone modifiche al piano sulla base delle mancanze riscontrate. La funzione di revisione interna controlla altresì i piani di continuità operativa dei fornitori di servizi e dei fornitori critici; essa può decidere di fare affidamento sulle strutture di questi ultimi se ritenute professionali e indipendenti quanto ai risultati dei controlli ed esamina i contratti per accertare che il livello di tutela sia adeguato agli obiettivi e agli standard aziendali;

— qualora nell'ambito della collaborazione e dello scambio di informazioni con il soggetto incaricato della revisione legale dei conti, viene a conoscenza di criticità emerse durante l'attività di revisione legale dei conti, si attiva affinché le competenti funzioni aziendali adottino i presidi necessari per superare tali criticità.

Con specifico riferimento al processo di gestione dei rischi, la funzione di revisione interna valuta anche:

— l'organizzazione, i poteri e le responsabilità della funzione di controllo dei rischi, anche con riferimento alla qualità e alla adeguatezza delle risorse a questa assegnate;

— l'appropriatezza delle ipotesi utilizzate nelle analisi di sensitività e di scenario e negli stress test;

— l'allineamento con le *best practice* diffuse nel settore.

Nello svolgimento dei propri compiti la funzione di revisione interna tiene conto di quanto previsto dagli standard professionali diffusamente accettati.

L'organizzazione della funzione di revisione interna è coerente con l'articolazione ed il grado di complessità della banca. Fermo restando che la funzione va posta alle dirette dipendenze dell'organo con funzione di supervisione strategica, vanno, tuttavia, preservati i raccordi con l'organo con funzione di gestione.

Indipendentemente dalle scelte organizzative, e fermo restando che i destinatari delle comunicazioni delle attività di verifica sono gli organi aziendali e le unità sottoposte a controllo, nella regolamentazione interna è espressamene previsto il potere per la funzione di revisione interna di comunicare in via diretta i risultati degli accertamenti e delle valutazioni agli organi aziendali. Gli esiti degli accertamenti conclusisi con giudizi negativi o che evidenzino carenze di rilievo sono trasmessi integralmente, tempestivamente e direttamente agli organi aziendali.

Per svolgere adeguatamente i propri compiti, la funzione di revisione interna ha accesso a tutte le attività, comprese quelle esternalizzate, della banca svolte sia presso gli uffici centrali sia presso le strutture periferiche. In caso di attribuzione a soggetti terzi di attività rilevanti per il funzionamento del sistema dei controlli interni (ad es., dell'attività di elaborazione dei dati), la funzione di revisione interna deve poter accedere anche alle attività svolte da tali soggetti.

3.5. *Rapporti tra le funzioni aziendali di controllo e altre funzioni aziendali.*

Fermo restando la reciproca indipendenza e i rispettivi ruoli, le funzioni aziendali di controllo collaborano tra loro e con le altre funzioni (ad es., funzione legale, organizzazione, sicurezza) allo scopo di sviluppare le proprie metodologie di controllo in modo coerente con le strategie e l'operatività aziendale.

Tenuto conto delle forti interrelazioni tra le diverse funzioni aziendali di controllo, specie tra le attività di controllo di conformità alle norme, di controllo dei rischi operativi e di revisione interna, è necessario che i compiti e le responsabilità delle diverse funzioni siano comunicati all'interno dell'organizzazione aziendale, in particolare per quanto attiene alla suddivisione delle competenze relative alla misurazione dei rischi, alla consulenza in materia di adeguatezza delle procedure di controllo nonché alle attività di verifica delle procedure medesime.

Specifica attenzione è posta nell'articolazione dei flussi informativi tra le funzioni aziendali di controllo; in particolare, i responsabili della funzione di controllo dei rischi e della funzione di conformità alle norme informano il responsabile della funzione di revisione interna delle criticità rilevate nelle proprie attività di controllo che possano essere di interesse per l'attività di *audit*. Il responsabile della revisione interna informa i responsabili delle altre funzioni aziendali di controllo per le eventuali inefficienze, punti di debolezza o irregolarità emerse nel corso delle attività di verifica di propria competenza e riguardanti specifiche aree o materie di competenza di queste ultime.

Sezione IV
ESTERNALIZZAZIONE DI FUNZIONI AZIENDALI (*OUTSOURCING*) AL DI FUORI DEL GRUPPO BANCARIO

1. Principi generali e requisiti particolari.

Le banche che ricorrono all'esternalizzazione di funzioni aziendali presidiano i rischi derivanti dalle scelte effettuate e mantengono la capacità di controllo e la responsabilità sulle attività esternalizzate nonché le competenze tecniche e gestionali essenziali per re-internalizzare, in caso di necessità, il loro svolgimento.

La decisione di ricorrere all'*outsourcing* per lo svolgimento di determinate funzioni aziendali (anche non importanti) è coerente con la politica aziendale in materia di esternalizzazione.

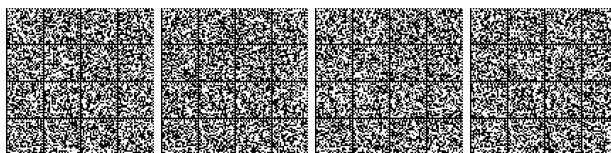
In linea con il principio di proporzionalità, tale politica stabilisce almeno:

— il processo decisionale per esternalizzare funzioni aziendali (livelli decisionali; funzioni coinvolte; valutazione dei rischi, inclusi quelli connessi con potenziali conflitti di interesse del fornitore di servizi, e l'impatto sulle funzioni aziendali; valutazione dell'impatto in termini di continuità operativa; criteri per la scelta e la *due diligence* del fornitore);

— il contenuto minimo dei contratti di *outsourcing* e i livelli di servizio attesi delle attività esternalizzate;

— le modalità di controllo, nel continuo e con il coinvolgimento della funzione di revisione interna, delle funzioni esternalizzate;

— i flussi informativi interni volti ad assicurare agli organi aziendali e alle funzioni aziendali di controllo la piena conoscenza e governabilità dei fattori di rischio relativi alle funzioni esternalizzate;

— i piani di continuità operativa (clausole contrattuali, piani operativi, ecc.) in caso di non corretto svolgimento delle funzioni esternalizzate da parte del fornitore di servizi.

La banca, attraverso il ricorso all'esternalizzazione, non può:

— delegare le proprie responsabilità, né la responsabilità degli organi aziendali. In linea con questo principio, a titolo esemplificativo, non è ammessa l'esternalizzazione di attività che rientrano tra i compiti degli organi aziendali (*cfr.* Sezione II) o che riguardano aspetti nevralgici del processo di erogazione del credito (ad es., il processo di valutazione del merito di credito e di monitoraggio delle relazioni creditizie); l'esternalizzazione delle funzioni aziendali di controllo è consentita nei limiti e alle condizioni previsti nel par. 2;

— alterare il rapporto e gli obblighi nei confronti dei suoi clienti;

— mettere a repentaglio la propria capacità di rispettare gli obblighi previsti dalla disciplina di vigilanza né mettersi in condizione di violare le riserve di attività previste dalla legge;

— pregiudicare la qualità del sistema dei controlli interni;

— ostacolare la vigilanza.

Ferma restando l'esigenza di assicurare, per ogni tipologia di esternalizzazione, il corretto svolgimento della stessa da parte del fornitore, il buon funzionamento del sistema dei controlli interni e il monitoraggio continuo dell'attività svolta dal fornitore di servizi, nel caso in cui intendano esternalizzare funzioni operative importanti le banche assicurano che siano soddisfatte le seguenti condizioni:

— nell'accordo scritto tra la banca e il fornitore di servizi sono formalizzati e chiaramente definiti:

a) i rispettivi diritti e obblighi; i livelli di servizio attesi, espressi in termini oggettivi e misurabili, nonché le informazioni necessarie per la verifica del loro rispetto; gli eventuali conflitti di interesse e le opportune cautele per prevenirli o, se non possibile, attenuarli; le condizioni al verificarsi delle quali possono essere apportate modifiche all'accordo; la durata dell'accordo e le modalità di rinnovo nonché gli impegni reciproci connessi con l'interruzione del rapporto;

b) i livelli di servizio assicurati in caso di emergenza e le soluzioni di continuità compatibili con le esigenze aziendali e coerenti con le prescrizioni dell'Autorità di vigilanza. Sono altresì stabilite le modalità di partecipazione, diretta o per il tramite di comitati utente, alle verifiche dei piani di continuità operativa dei fornitori.

Sono inoltre previste clausole risolutive espresse che consentano alla banca di porre termine all'accordo di esternalizzazione in presenza di eventi che possano compromettere la capacità del fornitore di garantire il servizio oppure quando si verifichi il mancato rispetto del livello di servizio concordato;

— il fornitore di servizi:

a) dispone della competenza, della capacità e delle autorizzazioni richieste dalla legge per esercitare, in maniera professionale e affidabile, le funzioni esternalizzate;

b) informa la banca di qualsiasi evento che potrebbe incidere sulla sua capacità di svolgere le funzioni esternalizzate in maniera efficace e in conformità con la normativa vigente; in particolare, comunica tempestivamente il verificarsi di incidenti di sicurezza, anche al fine di consentire la pronta attivazione delle relative procedure di gestione o di emergenza;

c) garantisce la sicurezza delle informazioni relative all'attività della banca, sotto l'aspetto della disponibilità, integrità e riservatezza; in quest'ambito, assicura il rispetto delle norme sulla protezione dei dati personali;

— la banca:

a) conserva la competenza richiesta per controllare efficacemente le funzioni esternalizzate e per gestire i rischi connessi con l'esternalizzazione, inclusi quelli derivanti da potenziali conflitti di interessi del fornitore di servizi; in tale ambito, individua, all'interno della propria organizzazione, un responsabile del controllo delle singole funzioni esternalizzate dotato di adeguati requisiti di professionalità («referente per le attività esternalizzate»);

b) acquisisce i piani di continuità operativa del fornitore di servizi o dispone di informazioni adeguate, al fine di valutare la qualità delle misure previste e di integrarle con le soluzioni di continuità realizzate all'interno;

— la banca, i suoi soggetti incaricati della revisione legale dei conti e le Autorità di vigilanza hanno effettivo accesso ai dati relativi alle attività esternalizzate e ai locali in cui opera il fornitore di servizi. Il diritto di accesso per l'Autorità di vigilanza deve risultare espressamente nel contratto, senza oneri aggiuntivi per l'intermediario;

— la sub-esternalizzazione (ovverosia la possibilità del fornitore di esternalizzare a sua volta una parte delle attività oggetto del contratto di esternalizzazione) non deve mettere a repentaglio il rispetto dei principi e delle condizioni per l'esternalizzazione previste nella presente disciplina; a tal fine, il contratto con il fornitore di servizi prevede che eventuali rapporti di sub-esternalizzazione siano preventivamente concordati con la banca e siano definiti in modo da consentire il pieno rispetto di tutte le condizioni sopra elencate relative al contratto primario, inclusa la possibilità per l'Autorità di vigilanza di avere accesso ai dati relativi alle attività esternalizzate e ai locali in cui opera il sub-fornitore di servizi.

2. Esternalizzazione delle funzioni aziendali di controllo.

L'esternalizzazione delle funzioni aziendali di controllo a soggetti terzi (19) dotati di requisiti idonei in termini di professionalità e indipendenza è ammessa, di norma, per le sole banche classificate, a fini SREP, nella macro-categoria 4 (20).

In aggiunta a quanto previsto dal par. 1 e dalla Sezione III, le banche che intendono esternalizzare, in tutto o in parte, le funzioni aziendali di controllo definiscono nell'accordo di esternalizzazione:

— gli obiettivi, la metodologia e la frequenza dei controlli;

— le modalità e la frequenza della reportistica dovuta al referente per l'attività esternalizzata e agli organi aziendali sulle verifiche effettuate. Resta fermo l'obbligo di dare riscontro tempestivamente a qualsiasi richiesta di informazioni e consulenza da parte di questi ultimi che in ogni caso rimangono responsabili del corretto espletamento delle attività di controllo esternalizzate;

— gli obblighi di riservatezza delle informazioni acquisite nell'esercizio della funzione;

— i collegamenti con le attività svolte dall'organo con funzione di controllo;

— la possibilità di richiedere specifiche attività di controllo al verificarsi di esigenze improvvise;

— la proprietà esclusiva della banca dei risultati dei controlli.

In linea con quanto previsto dal par. 1, la banca nomina specifici referenti per ciascuna delle singole funzioni aziendali di controllo esternalizzate Ai referenti per le funzioni aziendali di controllo esternalizzate si applicano le disposizioni previste dalla Sezione III, par. 1, lett. *b)*. Può essere nominato un unico referente per le funzioni aziendali di controllo di secondo livello esternalizzate.

Il fornitore di servizi presso cui si intendono esternalizzare le funzioni aziendali di controllo rispetta le seguenti condizioni (21):

— è indipendente rispetto alla banca presso la quale assume l'incarico;

— non cumula incarichi relativi a funzioni aziendali di controllo di secondo e di terzo livello per una stessa banca o gruppo bancario;

— non svolge contemporaneamente, per la stessa banca o gruppo bancario, incarichi relativi a funzioni aziendali di controllo e attività che sarebbe chiamato a controllare in qualità di fornitore di servizi;

— non svolge la funzione di revisione legale dei conti per la banca che esternalizza o per altre società del gruppo di appartenenza.

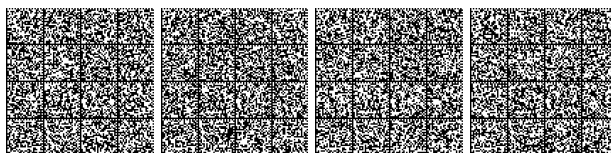
Nel rispetto delle medesime condizioni, inoltre, le banche, se in linea con il principio di proporzionalità, possono esternalizzare specifici controlli, che richiedono conoscenze professionali specializzate, in aree operative di contenute dimensioni e/o rischiosità.

3. Comunicazioni alla Banca d'Italia.

Le banche che intendono esternalizzare, in tutto o in parte, lo svolgimento di funzioni operative importanti o di controllo ne danno comunicazione preventiva alla Banca d'Italia. La comunicazione, corredata di tutte le indicazioni utili a verificare il rispetto dei criteri indicati nella presente Sezione, è effettuata almeno 60 giorni prima di conferire l'incarico e specifica le esigenze aziendali che hanno determinato la scelta. Entro 60 giorni dal ricevimento della comunicazione la Banca d'Italia può avviare un procedimento amministrativo d'ufficio di divieto dell'esternalizzazione che si conclude entro 60 giorni.

(19) Per soggetti terzi si intendono altre banche, società di revisione, ovvero gli organismi associativi di categoria (ad es., Federazioni regionali delle banche di credito cooperativo).

(20) Cfr. Circolare 269 del 7 maggio 2008, «Guida per l'attività di vigilanza», Sezione I, Capitolo I.5.

(21) Nel caso di esternalizzazione presso associazioni di categoria, la Banca d'Italia può ammettere l'adozione di presidi organizzativi equivalenti alle condizioni elencate.

Entro il 30 aprile di ogni anno le banche trasmettono alla Banca d'Italia una relazione, redatta dalla funzione di revisione interna — o, se esternalizzata, dal referente aziendale — con le considerazioni dell'organo con funzione di controllo e approvata dall'organo con funzione di supervisione strategica, relativa ai controlli svolti sulle funzioni operative importanti o di controllo esternalizzate, alle carenze eventualmente riscontrate e alle conseguenti azioni correttive adottate.

4. Esternalizzazione del trattamento del contante.

Fatta salva l'applicazione delle disposizioni in materia di esternalizzazione di funzioni operative importanti della presente Sezione e al fine di minimizzare i rischi operativi, in particolare di natura legale, e reputazionali connessi con l'eventuale erogazione alla clientela di banconote false o di qualità tale da non renderle idonee alla circolazione, le banche che esternalizzano l'attività di trattamento del contante adottano specifiche cautele nella gestione dei rapporti con i soggetti cui l'attività è esternalizzata sia all'atto della scelta del contraente, che deve fondarsi sull'accertamento della sua piena affidabilità, della correttezza della gestione e dell'adeguatezza delle strutture e dei processi organizzativi, sia nell'esercizio di efficaci controlli successivi, da svolgere nel continuo per verificare l'ordinato e corretto svolgimento dell'attività, nel pieno rispetto delle norme vigenti.

In particolare, le funzioni aziendali di controllo effettuano, ciascuna per i profili di competenza, una specifica valutazione delle procedure seguite per l'allacciamento e la gestione dei rapporti con i soggetti cui è esternalizzata l'attività di trattamento del contante nonché del complessivo assetto dei controlli sulle attività esternalizzate. Inoltre, tali funzioni assicurano il rispetto degli obblighi previsti dalla Decisione della Banca Centrale Europea del 16 settembre 2010, n. 14 relativa al controllo dell'autenticità e idoneità delle banconote in euro e al loro ricircolo.

La banca che intende esternalizzare l'attività di trattamento del contante stipula con il fornitore di servizi un contratto concluso in forma scritta che, oltre a rispettare i requisiti previsti nel paragrafo precedente, prevede:

— l'obbligo di attenersi alle disposizioni comunitarie sopra richiamate, con particolare riguardo: *(i)* all'utilizzo esclusivo di apparecchiature conformi a detta disciplina; *(ii)* alle procedure di verifica delle apparecchiature; *(iii)* alle attività di monitoraggio che possono essere condotte dalla Banca d'Italia;

— la possibilità per le banche di verificare la performance del servizio reso e di richiedere eventuali misure correttive;

— il diritto per la banca di recedere, senza penalità, nel caso in cui la controparte violi gli obblighi contrattuali e non vi ponga rimedio entro il periodo di tempo indicato nel contratto stesso.

Sezione V
IL RAF, IL SISTEMA DEI CONTROLLI INTERNI E L'ESTERNALIZZAZIONE NEI GRUPPI BANCARI

1. Il RAF nei gruppi bancari.

La capogruppo definisce e approva il RAF di gruppo secondo le indicazioni contenute nell'Allegato C, in quanto compatibili, assicurando la coerenza tra l'operatività, la complessità e le dimensioni del gruppo e il RAF stesso.

Il RAF di gruppo tiene conto delle specifiche operatività e dei connessi profili di rischio di ciascuna delle società componenti il gruppo in modo da risultare integrato e coerente. Per il conseguimento di tale obiettivo è necessario che gli organi aziendali della capogruppo svolgano i compiti loro affidati con riferimento non soltanto alla propria realtà aziendale ma anche valutando l'operatività complessiva del gruppo e i rischi cui esso è esposto.

Gli organi aziendali delle società componenti il gruppo, secondo le rispettive competenze, agiscono in coerenza con il RAF di gruppo e sono responsabili della sua attuazione per quanto concerne gli aspetti relativi alla propria realtà aziendale. A tal fine, è necessario che la capogruppo renda partecipi, nei modi ritenuti più opportuni, gli organi aziendali delle controllate delle scelte effettuate in materia di RAF.

2. Controlli interni di gruppo.

La capogruppo, nel quadro dell'attività di direzione e coordinamento del gruppo, esercita:

a) un *controllo strategico* sull'evoluzione delle diverse aree di attività in cui il gruppo opera e dei rischi incombenti sulle attività esercitate. Si tratta di un controllo sia sull'andamento delle attività svolte dalle società appartenenti al gruppo (crescita o riduzione per via endogena), sia sulle politiche di acquisizione e dismissione da parte delle società del gruppo (crescita o riduzione per via esogena);

b) un *controllo gestionale* volto ad assicurare il mantenimento delle condizioni di equilibrio economico, finanziario e patrimoniale sia delle singole società, sia del gruppo nel suo insieme. Queste esigenze di controllo vanno soddisfatte preferibilmente attraverso la predisposizione di piani, programmi e budget (aziendali e di gruppo), e mediante l'analisi delle situazioni periodiche, dei conti infra-annuali, dei bilanci di esercizio delle singole società e di quelli consolidati; ciò sia per settori omogenei di attività sia con riferimento all'intero gruppo;

c) un *controllo tecnico-operativo* finalizzato alla valutazione dei vari profili di rischio apportati al gruppo dalle singole controllate e dei rischi complessivi del gruppo.

La capogruppo che esercita l'attività di direzione e coordinamento in violazione dei principi di corretta gestione societaria e imprenditoriale è responsabile ai sensi degli artt. 2497 e ss. del codice civile.

La capogruppo dota il gruppo di un sistema unitario di controlli interni che consenta l'effettivo controllo sia sulle scelte strategiche del gruppo nel suo complesso sia sull'equilibrio gestionale delle singole componenti.

Per definire il sistema dei controlli interni del gruppo bancario, la capogruppo applica, per quanto compatibili, le disposizioni previste nelle precedenti Sezioni. A livello di gruppo — tenendo conto delle disposizioni in materia di organizzazione e controllo dei soggetti diversi dalle banche — vanno anche stabiliti e definiti:

— procedure formalizzate di coordinamento e collegamento fra le società appartenenti al gruppo e la capogruppo per tutte le aree di attività;

— compiti e responsabilità degli organi e delle funzioni di controllo all'interno del gruppo, le procedure di coordinamento, i riporti organizzativi, i flussi informativi e i relativi raccordi; a tali fini, l'organo con funzione di supervisione strategica della capogruppo approva un apposito documento di coordinamento dei controlli nell'ambito del gruppo. La relazione che le funzioni aziendali di controllo della capogruppo devono presentare agli organi aziendali (*cfr.* Sezione III, par. 2) illustra le verifiche effettuate, i risultati emersi, i punti di debolezza rilevati con riferimento, oltre che alla capogruppo medesima, anche al gruppo bancario nel suo complesso e propone gli interventi da adottare per la rimozione delle carenze rilevate;

— meccanismi di integrazione dei sistemi informativi e dei processi di gestione dei dati (specie per le società appartenenti al gruppo aventi sede in paesi che adottano diversi schemi/criteri contabili o di rilevazione), anche al fine di garantire l'affidabilità delle rilevazioni su base consolidata;

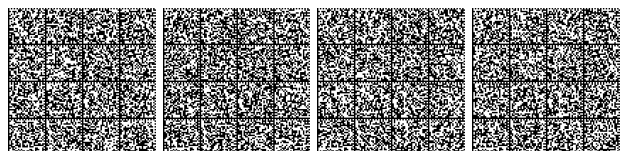
— flussi informativi periodici che consentano l'effettivo esercizio delle varie forme di controllo su tutte le componenti del gruppo;

— procedure che garantiscano, a livello accentrato, un efficace processo unitario di gestione dei rischi del gruppo a livello consolidato. In particolare, vi deve essere un'anagrafe unica, o più anagrafi che siano facilmente raccordabili, presso le diverse società del gruppo in modo da consentire l'univoca identificazione, da parte delle diverse entità, dei singoli clienti e controparti, dei gruppi di clienti connessi e dei soggetti collegati e rilevare correttamente, a livello consolidato, la loro esposizione complessiva ai diversi rischi;

— sistemi per monitorare i flussi finanziari, le relazioni di credito (in particolare le prestazioni di garanzie) e le altre relazioni fra i soggetti componenti il gruppo;

— controlli sul raggiungimento degli obiettivi di sicurezza informatica e di continuità operativa definiti per l'intero gruppo e le singole componenti.

L'organo con funzione di controllo della società capogruppo vigila anche sul corretto esercizio delle attività di controllo svolte dalla capogruppo sulle società del gruppo.

La capogruppo formalizza e rende noti a tutte le società del gruppo i criteri che presiedono le diverse fasi che costituiscono il processo di gestione dei rischi. Essa, inoltre, convalida i processi di gestione dei

rischi all'interno del gruppo. Per quanto riguarda in particolare il rischio di credito, la capogruppo fissa i criteri di valutazione delle posizioni e crea una base informativa comune che consenta a tutte le società appartenenti al gruppo di conoscere l'esposizione dei clienti nei confronti del gruppo nonché le valutazioni inerenti alle posizioni dei soggetti affidati. La capogruppo decide, infine, in merito all'adozione dei sistemi interni di misurazione dei rischi per la determinazione dei requisiti patrimoniali e ne determina le caratteristiche essenziali, assumendosi la responsabilità della realizzazione del progetto nonché della supervisione sul corretto funzionamento di tali sistemi e sul loro costante adeguamento sotto il profilo metodologico, organizzativo e procedurale.

Ciascuna società del gruppo si dota di un sistema dei controlli interni che sia coerente con la strategia e la politica del gruppo in materia di controlli, fermo restando il rispetto della disciplina eventualmente applicabile su base individuale.

Nel caso di controllate estere, è necessario che la capogruppo, nel rispetto dei vincoli locali, adotti tutte le iniziative atte a garantire standard di controllo e presidi comparabili a quelli previsti dalle disposizioni di vigilanza italiane, anche nei casi in cui la normativa dei paesi in cui sono insediate le filiazioni non preveda analoghi livelli di attenzione.

Per verificare la rispondenza dei comportamenti delle società appartenenti al gruppo agli indirizzi della capogruppo nonché l'efficacia del sistema dei controlli interni, la capogruppo si attiva affinché, nei limiti dell'ordinamento, la funzione di revisione interna a livello consolidato effettui periodicamente verifiche in loco sulle componenti del gruppo, tenuto conto della rilevanza delle diverse tipologie di rischio assunte dalle diverse entità.

3. Esternalizzazione di funzioni aziendali all'interno del gruppo bancario.

La capogruppo definisce la politica aziendale in materia di esternalizzazione all'interno del gruppo bancario.

La politica stabilisce almeno:

— il processo decisionale per esternalizzare funzioni aziendali presso la capogruppo o altre componenti del gruppo;

— i presidi adottati per assicurare una adeguata tutela degli interessi di eventuali soci di minoranza;

— i criteri per individuare il fornitore di servizi all'interno del gruppo, e gli obblighi previsti per tale soggetto; in particolare, con riferimento alle funzioni operative importanti, il fornitore di servizi:

a) dispone della competenza, della capacità e delle autorizzazioni richieste dalla legge per esercitare, in maniera professionale e affidabile, le funzioni esternalizzate;

b) informa la capogruppo e la banca che esternalizza di qualsiasi evento che potrebbe incidere sulla sua capacità di svolgere le funzioni esternalizzate in maniera efficace e in conformità con la normativa vigente;

c) comunica tempestivamente il verificarsi di incidenti di sicurezza, anche al fine di consentire la pronta attivazione delle relative procedure di gestione o di emergenza;

d) garantisce la sicurezza delle informazioni relative all'attività della banca che esternalizza, sotto l'aspetto della disponibilità, integrità e riservatezza; in quest'ambito, assicura il rispetto delle norme sulla protezione dei dati personali;

— il contenuto minimo dei contratti di *outsourcing* e i livelli di servizio attesi delle attività esternalizzate;

— i livelli di servizio assicurati in caso di emergenza e le soluzioni di continuità compatibili con le esigenze aziendali e coerenti con le prescrizioni dell'Autorità di vigilanza;

— i flussi informativi volti ad assicurare agli organi aziendali della capogruppo e della banca che esternalizza e alle funzioni aziendali di controllo di tali soggetti la piena conoscenza e governabilità dei fattori di rischio relativi alle funzioni esternalizzate.

La banca appartenente a un gruppo bancario, ferma restando la responsabilità per le attività esternalizzate, può derogare alle disposizioni in materia di esternalizzazione previste alla Sezione IV se rispetta la politica aziendale in materia di esternalizzazione all'interno del gruppo. Attraverso il ricorso all'esternalizzazione, la banca non può:

— delegare le proprie responsabilità, né la responsabilità degli organi aziendali. In linea con questo principio, a titolo esemplificativo, non è ammessa l'esternalizzazione di attività che rientrano tra i compiti degli organi aziendali (*cfr.* Sezione II);

— alterare il rapporto e gli obblighi nei confronti dei suoi clienti;

— mettere a repentaglio la propria capacità di rispettare gli obblighi previsti dalla disciplina di vigilanza né mettersi in condizione di violare le riserve di attività previste dalla legge;

— pregiudicare la qualità del sistema dei controlli interni, tenuto conto dell'assetto complessivo dei controlli del gruppo di appartenenza;

— ostacolare la vigilanza.

3.1. *L'esternalizzazione nell'ambito del gruppo delle funzioni aziendali di controllo.*

Fermo restando quanto previsto nel par. 3, al fine di assicurare l'effettività e l'integrazione dei controlli, l'esternalizzazione delle funzioni aziendali di controllo presso la capogruppo o le altre componenti del gruppo è consentita, indipendentemente dalle dimensioni e dalla complessità operativa della banca, nel rispetto dei seguenti criteri:

— sono valutati e documentati, in una logica di gruppo, i costi, i benefici e i rischi alla base della soluzione adottata; tale analisi deve essere periodicamente aggiornata;

— gli organi aziendali delle componenti del gruppo sono consapevoli delle scelte effettuate dalla capogruppo e sono responsabili, ciascuno secondo le proprie competenze, dell'attuazione, nell'ambito delle rispettive realtà aziendali, delle strategie e politiche perseguite in materia di controlli, favorendone l'integrazione nell'ambito dei controlli di gruppo;

— all'interno delle banche del gruppo e delle altre entità che, a giudizio della capogruppo, assumono rischi considerati rilevanti per il gruppo nel suo complesso, vengono nominati appositi referenti i quali: *i)* svolgono compiti di supporto per la funzione aziendale di controllo esternalizzata; *ii)* riportano funzionalmente alla funzione aziendale di controllo esternalizzata; *iii)* segnalano tempestivamente eventi o situazioni particolari, suscettibili di modificare i rischi generati dalla controllata (22). A tali referenti si applicano le disposizioni previste dalla Sezione III, par. 1, lett. *b)*. Può essere nominato un unico referente per le sole funzioni aziendali di controllo di secondo livello esternalizzate.

4. Comunicazioni alla Banca d'Italia.

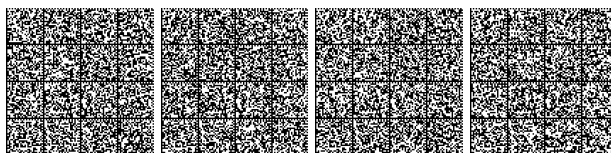
Le banche che intendono esternalizzare, in tutto o in parte, lo svolgimento di funzioni operative importanti o di controllo nell'ambito del gruppo di appartenenza ne danno comunicazione preventiva alla Banca d'Italia, tramite la propria capogruppo. La comunicazione, corredata di tutte le indicazioni utili a verificare il rispetto dei criteri indicati nella presente Sezione, è effettuata almeno 60 giorni prima di conferire l'incarico e specifica le esigenze aziendali che hanno determinato la scelta. Entro 60 giorni dal ricevimento della comunicazione la Banca d'Italia può avviare un procedimento amministrativo d'ufficio di divieto dell'esternalizzazione che si conclude entro 60 giorni.

La capogruppo, sulla base delle relazioni delle funzioni aziendali di controllo (*cfr.* Sezione III, par. 2 e par. 2 della presente Sezione), invia annualmente alla Banca d'Italia una relazione riguardante gli accertamenti effettuati sulle società controllate e i risultati emersi, i punti di debolezza rilevati con riferimento sia al gruppo bancario nel suo complesso sia alle singole entità e la descrizione degli interventi da adottare per la rimozione delle carenze rilevate.

Sezione VI
IMPRESE DI RIFERIMENTO

Le imprese di riferimento sono responsabili del calcolo dei requisiti patrimoniali e del rispetto delle disposizioni prudenziali applicabili su base consolidata (23); a tali fini, il sistema di controlli interni nel suo complesso assicura la correttezza, l'adeguatezza e la tempestività dei flussi informativi con le altre società bancarie, finanziarie e strumentali controllate dalla società di partecipazione finanziaria madre nell'UE necessari per rispettare gli obblighi imposti dalle disposizioni prudenziali.

(22) A seconda della funzione aziendale di controllo esternalizzata può trattarsi di responsabili di unità di controllo del rischio locali, compliance officer, responsabili di unità distaccate di internal audit.

(23) Cfr. Titolo I, Capitolo 1, Sezione III, par. 1.

Sezione VII

SUCCURSALI DI BANCHE COMUNITARIE E DI BANCHE EXTRACOMUNITARIE AVENTI SEDE NEI PAESI DEL GRUPPO DEI DIECI O IN QUELLI INCLUSI IN UN ELENCO PUBBLICATO DALLA BANCA D'ITALIA

Nel caso delle succursali di banche comunitarie e delle succursali di banche extracomunitarie aventi sede nei paesi del Gruppo dei Dieci ovvero in quelli inclusi in un elenco pubblicato e periodicamente aggiornato dalla Banca d'Italia, il legale rappresentante attesta annualmente che è stata condotta una verifica di conformità della condotta aziendale rispetto alle norme italiane applicabili alla succursale e riferisce sinteticamente alla Banca d'Italia in merito all'esito di tale verifica (24).

A tal fine, la banca verifica che le procedure interne adottate dalla succursale stessa siano adeguate rispetto all'obiettivo di prevenire la violazione delle norme italiane applicabili alla succursale.

Nel caso delle succursali di banche extracomunitarie aventi sede nei paesi del Gruppo dei Dieci ovvero in quelli inclusi in un elenco pubblicato e periodicamente aggiornato dalla Banca d'Italia, il legale rappresentante attesta altresì che la completezza, l'adeguatezza, la funzionalità, l'affidabilità del sistema dei controlli interni è stata verificata attraverso un processo di revisione interna.

Sezione VIII

INFORMATIVA ALLA BANCA D'ITALIA

Le banche comunicano tempestivamente alla Banca d'Italia la nomina e l'eventuale revoca dei responsabili delle funzioni aziendali di controllo. Nel caso di gruppi bancari tale comunicazione è eseguita dalla capogruppo.

Le banche non appartenenti a gruppi bancari trasmettono inoltre alla Banca d'Italia:

— tempestivamente, le relazioni sull'attività svolta redatte annualmente dalle funzioni di controllo dei rischi, di conformità alle norme e di revisione interna (*cfr.* Sezione III, par. 2). Se una o più di queste funzioni sono esternalizzate, la relazione è redatta dal referente aziendale;

— entro il 30 aprile di ogni anno, una relazione, redatta dalla funzione di revisione interna - o, se esternalizzata, dal referente aziendale - con le considerazioni dell'organo con funzione di controllo e approvata dall'organo con funzione di supervisione strategica, relativa ai controlli svolti sulle funzioni operative importanti esternalizzate, alle carenze eventualmente riscontrate e alle conseguenti azioni correttive adottate (*cfr.* Sezione IV, par. 3);

— qualora ve ne siano le condizioni, la relazione di cui al punto 2.1 dell'Allegato A.

Le banche non appartenenti a gruppi che intendono esternalizzare, in tutto o in parte, lo svolgimento di funzioni operative importanti o di controllo ne danno comunicazione preventiva alla Banca d'Italia (*cfr.* Sezione IV, par. 3).

Nel caso di gruppi bancari, le capogruppo coordinano e trasmettono alla Banca d'Italia, per tutte le banche del gruppo, la stessa documentazione richiesta nel caso delle banche non appartenenti a gruppi bancari, ad eccezione delle relazioni delle funzioni aziendali di controllo delle società controllate (Sezione III, par. 2). In luogo di queste ultime, inviano annualmente alla Banca d'Italia la relazione di cui alla Sezione V, par. 4, riguardante gli accertamenti effettuati sulle società controllate e i risultati emersi, i punti di debolezza rilevati con riferimento sia al gruppo bancario nel suo complesso sia alle singole entità e la descrizione degli interventi da adottare per la rimozione delle carenze rilevate.

Le capogruppo danno comunicazione preventiva alla Banca d'Italia dell'intenzione delle banche di esternalizzare, in tutto o in parte, lo svolgimento di funzioni operative importanti o di controllo nell'ambito del gruppo bancario di appartenenza (*cfr.* Sezione V, par. 4).

Nel caso delle succursali di banche comunitarie e delle succursali di banche extracomunitarie aventi sede nei paesi del Gruppo dei Dieci ovvero in quelli inclusi in un elenco pubblicato e periodicamente aggiornato dalla Banca d'Italia, il legale rappresentante attesta annualmente che è stata condotta una verifica di conformità della condotta aziendale rispetto alle norme italiane applicabili alla succursale e riferisce sinteticamente alla Banca d'Italia in merito all'esito di tale verifica (*cfr.* Sezione VII).

Nel caso delle succursali di banche extracomunitarie aventi sede nei paesi del Gruppo dei Dieci ovvero in quelli inclusi in un elenco pubblicato e periodicamente aggiornato dalla Banca d'Italia, il legale rappresentante attesta altresì che la completezza, l'adeguatezza, la funzionalità, l'affidabilità del sistema dei controlli interni è stata verificata attraverso un processo di revisione interna (*cfr.* Sezione VII).

Le succursali di banche extracomunitarie non aventi sede nei paesi del Gruppo dei Dieci ovvero in quelli inclusi in un elenco pubblicato e periodicamente aggiornato dalla Banca d'Italia, individuano un referente per ciascuna funzione aziendale di controllo della succursale. I nominativi dei referenti e le eventuali variazioni sono comunicati alla Banca d'Italia.

ALLEGATO A

DISPOSIZIONI SPECIALI RELATIVE
A PARTICOLARI CATEGORIE DI RISCHIO

1. Premessa.

Vengono in questa sede individuate disposizioni speciali in materia di controlli interni, che assumono valenza per la generalità delle banche e dei gruppi bancari, relativamente a specifiche categorie di rischio. Nel caso in cui la banca utilizzi sistemi interni di misurazione dei rischi per la determinazione dei requisiti patrimoniali (credito, controparte, mercato, operativi), queste indicazioni devono essere integrate con i principi di carattere organizzativo previsti dalle rispettive discipline, i quali costituiscono una delle condizioni per il riconoscimento, a fini prudenziali, di tali sistemi.

2. Rischio di credito e di controparte.

L'intero processo di gestione del rischio di credito e di controparte (misurazione del rischio, istruttoria, erogazione, controllo andamentale e monitoraggio delle esposizioni, revisione delle linee di credito, classificazione delle posizioni di rischio, interventi in caso di anomalia, criteri di classificazione, valutazione e gestione delle esposizioni deteriorate) deve risultare dal regolamento interno ed essere periodicamente sottoposto a verifica.

Nel definire i criteri per l'erogazione dei crediti, il regolamento interno assicura che la diversificazione dei vari portafogli esposti al rischio di credito sia coerente con gli obiettivi di mercato e la strategia complessiva della banca.

La corretta misurazione del rischio di credito presuppone che le banche abbiano in ogni momento conoscenza della propria esposizione verso ciascun cliente e verso ciascun gruppo di clienti connessi (con rilevanza sia delle connessioni di carattere giuridico sia di quelle di tipo economico-finanziario). A tale fine, è indispensabile la disponibilità di basi dati complete ed aggiornate, di un sistema informativo che ne consenta lo sfruttamento ai fini richiesti, di un'anagrafe clienti attraverso cui generare ed aggiornare, a livello individuale e, nel caso di un gruppo bancario, consolidato, i dati identificativi della clientela, le connessioni giuridiche ed economico-finanziarie tra clienti diversi, le forme tecniche da cui deriva l'esposizione, il valore aggiornato delle tecniche di attenuazione dei rischi.

La corretta rilevazione e gestione di tutte le informazioni necessarie riveste particolare importanza nelle procedure per l'assunzione di grandi rischi. A tal fine, le banche sono tenute al rispetto della disciplina dettata nel Titolo V, Capitolo 1, Sezione V.

Nella fase istruttoria, le banche acquisiscono tutta la documentazione necessaria per effettuare un'adeguata valutazione del merito di credito del prenditore, sotto il profilo patrimoniale e reddituale, e una corretta remunerazione del rischio assunto. La documentazione deve consentire di valutare la coerenza tra importo, forma tecnica e progetto finanziato; essa deve inoltre permettere l'individuazione delle caratteristiche e della qualità del prenditore, anche alla luce del complesso delle relazioni intrattenute. Nel caso di affidamenti ad imprese, sono acquisiti i bilanci (individuali e, se disponibili, consolidati), le altre informazioni desumibili dalla Centrale dei Bilanci e ogni altra informazione, significativa e rilevante, per valutare la situazione aziendale attuale e prospettica dell'impresa, anche di carattere qualitativo (validità del progetto imprenditoriale, assetti proprietari, esame della situazione del settore economico di appartenenza, situazione dei mercati di sbocco e di fornitura, ecc.). Le procedure di sfruttamento delle informazioni devono fornire indicazioni circostanziate sul livello di affidabilità del cliente

(24) L'attestato contiene almeno la descrizione sintetica: i) dell'attività svolta dalla succursale; ii) delle soluzioni organizzative adottate.

(ad es., attraverso sistemi di *credit scoring* e/o di *rating*). Nel caso in cui l'affidato faccia parte di un gruppo, la valutazione tiene conto anche della situazione e delle prospettive del gruppo nel suo complesso. Al fine di conoscere la valutazione degli affidati da parte del sistema bancario le banche utilizzano, anche nella successiva fase di controllo andamentale e monitoraggio delle esposizioni, le informazioni fornite dalla Centrale dei Rischi.

Le deleghe in materia di erogazione del credito devono risultare da apposita delibera dell'organo con funzione di supervisione strategica e devono essere commisurate alle caratteristiche dimensionali della banca. Nel caso di fissazione di limiti «a cascata» (quando, cioè, il delegato delega a sua volta entro i limiti a lui attribuiti), la griglia dei limiti risultanti deve essere documentata. Il soggetto delegante deve inoltre essere periodicamente informato sull'esercizio delle deleghe, al fine di poter effettuare le necessarie verifiche.

Il controllo andamentale e il monitoraggio delle singole esposizioni devono essere svolti con sistematicità, avvalendosi di procedure efficaci in grado di segnalare tempestivamente l'insorgere di anomalie e di assicurare l'adeguatezza delle rettifiche di valore e dei passaggi a perdita.

I criteri di classificazione, valutazione e gestione delle esposizioni deteriorate (25), nonché le relative unità responsabili devono essere stabiliti dall'organo con funzione di supervisione strategica con apposita delibera che indichi anche le modalità di raccordo tra tali criteri e quelli previsti per le segnalazioni di vigilanza. La deroga all'applicazione dei criteri prefissati è consentita esclusivamente in casi predeterminati e seguendo procedure rafforzate, che prevedano il coinvolgimento dell'organo con funzione di gestione. Devono essere altresì stabilite procedure atte a individuare, in dettaglio, gli interventi da attuare in presenza di deterioramento delle posizioni di rischio.

In particolare, la determinazione del valore di recupero dei crediti deteriorati tiene conto dei seguenti fattori: *i)* tipologia di procedura esecutiva attivata ed esito delle fasi già esperite; *ii)* valore di pronto realizzo delle garanzie (calcolando per i beni immobili *haircut* in funzione dell'aggiornamento della perizia e del contesto di mercato; per le attività finanziarie scarti coerenti con la natura del prodotto e la situazione di mercato); *iii)* criteri per la stima del periodo di recupero e dei tassi di attualizzazione dei flussi attesi. Le suddette indicazioni sono periodicamente aggiornate sulla base dell'evoluzione del quadro di riferimento.

La verifica del corretto svolgimento del monitoraggio andamentale sulle singole esposizioni, in particolare di quelle deteriorate, e la valutazione della coerenza delle classificazioni, della congruità degli accantonamenti e dell'adeguatezza del processo di recupero è svolta, a livello centrale e periferico, dalla funzione di controllo dei rischi o, per le banche di maggiore dimensione e complessità operativa, da una specifica unità, che riporta al responsabile della funzione di controllo dei rischi.

Tali unità verificano, tra l'altro, l'operato delle unità operative e di recupero crediti, assicurando la corretta classificazione delle esposizioni deteriorate e l'adeguatezza del relativo grado di irrecuperabilità (26). Nel caso di valutazioni discordanti, si applicano le valutazioni formulate dalla funzione di controllo dei rischi.

L'*internal audit* assicura periodiche verifiche sull'affidabilità ed efficacia del complessivo processo.

Gli organi aziendali, nell'ambito delle rispettive competenze, sono costantemente aggiornati dei risultati conseguiti nell'applicazione dei criteri e delle procedure individuate e valutano l'esigenza di definire interventi di miglioramento di tali criteri e procedure.

Il sistema dei controlli interni deve, infine, garantire che l'intero processo di gestione del rischio ricomprenda l'esposizione al rischio di credito derivante dall'operatività diversa dalla tipica attività di finanziamento, costituita dai derivati finanziari e di credito, dalle operazioni SFT («*securities financing transactions*») e da quelle con regolamento a lungo termine, così come definite nella disciplina relativa al trattamento prudenziale dei rischi di controparte.

A tal fine, le banche sono tenute anche al rispetto dei requisiti organizzativi per l'operatività in derivati di credito (27).

Nel caso di partecipazione ad accordi di compensazione, su base bilaterale o multilaterale, che misurano il rischio di controparte sulla base dell'esposizione netta anziché lorda, le banche verificano che gli accordi abbiano fondamento giuridico. Nel caso in cui i predetti accordi intendano riconoscere anche a fini prudenziali l'effetto di riduzione del rischio devono attenersi al rispetto dei criteri previsti dalla normativa (*cfr.* Titolo II, Capitolo 3, Sezione II, par. 10).

L'esigenza di assicurare idonei presidi non viene meno nei casi in cui i finanziamenti sono concessi nella forma del rilascio di garanzie, posto che il credito di firma concesso espone la banca al rischio di dover successivamente intervenire con una erogazione per cassa, attivando conseguentemente le azioni di recupero. Ciò in particolare quando il rilascio di garanzie costituisce l'attività esclusiva o prevalente della banca.

I presidi organizzativi devono pertanto assicurare anche:

— l'approfondita conoscenza — sin dall'inizio della relazione e per tutta la durata della stessa — della capacità dei garantiti di adempiere le proprie obbligazioni (incluse quelle di fare);

— il costante monitoraggio degli impegni assunti con riferimento sia al volume sia al grado di rischiosità degli stessi, specie in situazioni di elevata rotazione delle garanzie rilasciate.

Una particolare attenzione va inoltre posta nella definizione della contrattualistica, al fine di prevenire o limitare l'insorgere di contenziosi con riferimento sia all'attivazione delle garanzie rilasciate, sia alle successive eventuali azioni di rivalsa nei confronti dei garantiti.

Le banche si astengono dal sottoscrivere i contratti relativi alle garanzie rilasciate prima della definizione di tutti gli elementi essenziali del rapporto (in particolare: indicazione del beneficiario, prestazione dovuta dal garantito, ammontare e durata della garanzia, modalità di liberazione dall'obbligo di garanzia o di rinnovo della stessa).

Al fine di assicurare il monitoraggio dell'esposizione, anche per il rispetto dei requisiti prudenziali in presenza elevata rotazione delle garanzie, il sistema delle rilevazioni contabili aziendali deve consentire di ricostruire la successione temporale delle operazioni effettuate.

2.1. *Valutazione del merito di credito.*

Le disposizioni in materia di determinazione dei requisiti patrimoniali a fronte del rischio di credito nel metodo standardizzato, prevedono l'applicazione di coefficienti di ponderazione diversificati in funzione delle valutazioni del merito creditizio rilasciate dalle ECAI.

Il riconoscimento di un'ECAI, effettuato dalla Banca d'Italia mediante la procedura di cui al Titolo II, Capitolo 1, Parte Prima, Sezione VIII, non implica una valutazione di merito sulla validità dei giudizi attribuiti o un supporto alle metodologie utilizzate, di cui le ECAI restano le uniche responsabili; esso è volto a consentire alle banche l'utilizzo dei *rating* esterni ai fini del calcolo dei requisiti patrimoniali.

L'utilizzo dei rating esterni non esaurisce il processo di valutazione del merito di credito che le banche devono svolgere nei confronti della clientela sovvenuta; esso rappresenta soltanto uno degli elementi che possono contribuire alla definizione del quadro informativo sulla qualità creditizia del cliente.

Le banche si dotano, pertanto, di metodologie interne che consentano una valutazione del rischio di credito derivante da esposizioni nei confronti di singoli prenditori, titoli, posizioni verso le cartolarizzazioni nonché del rischio di credito a livello di portafoglio (28). Tali metodologie non devono basarsi meccanicamente sulle valutazioni espresse dalle ECAI.

La valutazione del merito di credito svolta dalla banca in base alle risultanze dell'attività istruttoria e delle sue metodologie interne può discostarsi da quelle effettuate dalle ECAI.

Divergenze frequenti nella valutazione del merito di credito possono essere indice di incompletezza e scarsa accuratezza del sistema di valutazione dell'agenzia esterna e costituiscono utili informazioni ai fini della periodica valutazione che la Banca d'Italia effettua sulla permanenza dei presupposti per il riconoscimento delle ECAI.

Le banche, oltre ad analizzare la qualità dei singoli prenditori nell'ambito del processo di gestione del rischio, sono tenute a effettuare, con periodicità almeno annuale, una specifica valutazione della

---

(25) Nei gruppi bancari i criteri di classificazione, valutazione e gestione devono essere applicati in maniera omogenea.

(26) I controlli dovranno riguardare tra l'altro: la presenza di aggiornati valori peritali delle garanzie; la registrazione nelle procedure automatiche di tutte le informazioni necessarie per la valutazione dei crediti; la tracciabilità del processo di recupero; le stime dei tempi di recupero e i tassi di attualizzazione utilizzati.

(27) Cfr. Bollettino di vigilanza n. 4 - Aprile 2006 (http://www.bancaditalia.it/vigilanza/pubblicazioni/bollvig/06/Bollvig_04_06.pdf).

(28) Le banche, in linea con il principio di proporzionalità, possono non sviluppare apposite metodologie per la valutazione interna del rischio di credito derivante dalle esposizioni verso amministrazioni centrali e banche centrali.

complessiva coerenza dei *rating* delle ECAI con le valutazioni elaborate in autonomia. I risultati dell'esame sono formalizzati in un documento approvato dall'organo con funzione di gestione e portato a conoscenza dell'organo con funzione di supervisione strategica e dell'organo con funzione di controllo. Ove dall'esame emergano frequenti e significativi disallineamenti fra valutazioni interne ed esterne, copia della citata relazione è trasmessa alla Banca d'Italia.

3. Rischi derivanti dall'utilizzo di tecniche di attenuazione del rischio di credito.

Requisiti organizzativi specifici per la gestione dei rischi derivanti dall'utilizzo di tecniche di attenuazione del rischio di credito sono contenute nel Titolo II, Capitolo 2, Parte Prima, Sezione II.

4. Concentrazione dei rischi.

Regole organizzative specifiche in materia di grandi rischi sono contenute nel Titolo V, Capitolo 1, Sezione V.

Inoltre, il sistema dei controlli interni assicura la gestione e il controllo, anche attraverso specifiche politiche e procedure aziendali, dei rischi di concentrazione derivanti dalle esposizioni nei confronti di clienti, incluse le controparti centrali, gruppi di clienti connessi, clienti operanti nel medesimo settore economico, nella medesima regione geografica o che esercitano la stessa attività o trattano la stessa merce nonché dall'applicazione di tecniche di attenuazione del rischio di credito, compresi in particolare i rischi derivanti da esposizioni indirette come, ad esempio, nei confronti di singoli fornitori di garanzie (*cfr*. Titolo III, Capitolo 1, Allegato B).

5. Rischi derivanti da operazioni di cartolarizzazione.

Regole organizzative specifiche in materia di operazioni di cartolarizzazione sono contenute nel Titolo II, Capitolo 2, Parte Seconda, Sezione VII.

In particolare, il sistema dei controlli interni assicura che i rischi derivanti da tali operazioni inclusi i rischi reputazionali derivanti, ad esempio, dall'utilizzo di strutture o prodotti complessi, siano gestiti e valutati attraverso adeguate politiche e procedure volte a garantire che la sostanza economica di dette operazioni sia pienamente in linea con la loro valutazione di rischiosità e con le decisioni degli organi aziendali.

6. Rischi di mercato.

I principali requisiti relativi al processo di gestione dei rischi di mercato sono riportati nel Titolo II, Capitolo 4.

Il sistema di controlli interni, in particolare, assicura l'attuazione di politiche e procedure volte a identificare, misurare e gestire tutte le fonti e gli effetti derivanti dall'esposizione a rischi di mercato.

Nei casi in cui una posizione corta abbia scadenza inferiore rispetto alla relativa posizione lunga, la banca adotta adeguati presidi volti a prevenire il rischio di liquidità.

In ogni caso, le banche che non sono in grado di misurare e gestire correttamente i rischi associati a strumenti finanziari sensibili a più fattori di rischio devono astenersi dalla negoziazione di tali strumenti (*cfr*. Titolo II, Capitolo 4, Parte Seconda, Sezione II).

7. Rischio tasso di interesse derivante da attività non appartenenti al portafoglio di negoziazione a fini di vigilanza.

Le banche predispongono adeguati sistemi volti a identificare, valutare e gestire i rischi derivanti da potenziali variazioni del livello dei tassi di interesse riguardanti attività non appartenenti al portafoglio di negoziazione a fini di vigilanza (*cfr*. Titolo III, Capitolo 1, Allegato C).

8. Rischi operativi.

Diversamente dagli altri rischi di «primo pilastro», per i quali la banca, in base alla sua propensione al rischio, assume consapevolmente posizioni creditizie o finanziarie per raggiungere il desiderato profilo di rischio/rendimento, l'assunzione di rischi operativi risulta implicita nella decisione di intraprendere un determinato tipo di attività e, più in generale, nello svolgimento dell'attività d'impresa.

In tale contesto, il sistema dei controlli interni deve costituire il presidio principale per la prevenzione ed il contenimento di tali rischi. In particolare, devono essere approvate e attuate politiche e procedure aziendali volte a definire, identificare, valutare e gestire l'esposizione ai rischi operativi, inclusi quelli derivanti da eventi caratterizzati da bassa frequenza e particolare gravità.

Le disposizioni in materia di governo e gestione dei rischi operativi sono riportate nel Titolo II, Capitolo 5. Esse si differenziano in relazione al tipo di trattamento prudenziale adottato dalla banca.

Le banche, inoltre, applicano le linee guida del CEBS/EBA in materia di gestione dei rischi operativi derivanti dall'attività di *trading* (*cfr*. CEBS/EBA GL35, «*Guidelines on management of operational risks in market-related activities*»).

9. Rischio di liquidità.

Considerata l'importanza crescente che il rischio di liquidità ha assunto nel corso del tempo, i principi e le linee guida del sistema dei controlli interni sono trattati nel più ampio contesto dei presidi organizzavi da predisporre a fronte di questa categoria di rischio (Titolo V, Capitolo 2, Sezione V).

10. Rischio di leva finanziaria eccessiva.

Le banche si dotano di politiche e procedure aziendali volte a identificare, gestire e monitorare il rischio di eccessiva leva finanziaria. Indicatori di tale tipologia di rischio sono l'indice di leva finanziaria e i disallineamenti tra attività e passività.

Le banche gestiscono conservativamente il rischio di eccessiva leva finanziaria considerando i potenziali incrementi di tale rischio dovuti alle riduzioni dei fondi propri della banca causate da perdite attese o realizzate derivanti dalle regole contabili applicabili. A tal fine, le banche devono essere in grado di far fronte a diverse situazioni di stress con riferimento al rischio di leva finanziaria eccessiva.

11. Rischi connessi con l'emissione di obbligazioni bancarie garantite.

Regole di dettaglio in materia di responsabilità degli organi aziendali e controlli sulle banche che emettono obbligazioni bancarie garantite sono riportate nel Titolo V, Capitolo 3, Sezione II, par. 5.

12. Rischi connessi con l'assunzione di partecipazioni.

Al fine di gestire i rischi specifici connessi con l'assunzione di partecipazioni da parte di banche e gruppi bancari, specifiche regole organizzative e di governo societario sono contenute nel Titolo V, Capitolo 4, Sezione VII.

13. Attività di rischio e conflitti di interesse nei confronti di soggetti collegati.

Con specifico riferimento alle operazioni con parti correlate si applicano specifiche disposizioni in materia di controlli interni e responsabilità degli organi aziendali contenute nel Titolo V, Capitolo 5, Sezione IV.

14. Rischi connessi con l'attività di banca depositaria di OICR e fondi pensione.

Le banche che assumono l'incarico di depositaria rispettano le regole specifiche in materia di controlli interni contenute nel Titolo V, Capitolo 6, Sezioni II e IV.

15. Rischio paese e rischio di trasferimento (*Country and transfer risks*).

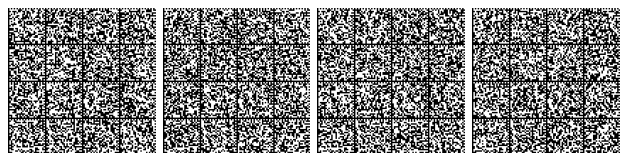
Le banche sono tenute a presidiare efficacemente, in linea con il principio di proporzionalità, il rischio paese (29) e il rischio di trasferimento (30).

In particolare, le banche, tengono conto di tali rischi nell'ambito del RAF, del processo per determinare il capitale complessivo adeguato in termini attuali e prospettici (ICAAP) (31) e del processo di gestione dei rischi.

---

(29) Il rischio paese è il rischio di perdite causate da eventi che si verificano in un paese diverso dall'Italia. Il concetto di rischio paese è più ampio di quello di rischio sovrano in quanto è riferito a tutte le esposizioni indipendentemente dalla natura delle controparti, siano esse persone fisiche, imprese, banche o amministrazioni pubbliche.

(30) Il rischio di trasferimento è il rischio che una banca, esposta nei confronti di un soggetto che si finanzia in una valuta diversa da quella in cui percepisce le sue principali fonti di reddito, realizzi delle perdite dovute alle difficoltà del debitore di convertire la propria valuta nella valuta in cui è denominata l'esposizione.

(31) Cfr. Titolo III, Capitolo 1, Sezione II - La valutazione aziendale dell'adeguatezza patrimoniale (ICAAP).

Le banche formalizzano criteri per la determinazione di accantonamenti adeguati a fronte delle singole esposizioni soggette ai rischi menzionati.

ALLEGATO B

CONTROLLI SULLE SUCCURSALI ESTERE

Le succursali estere di banche italiane presentano peculiari esigenze di controllo. Vengono di seguito formulate alcune indicazioni di carattere minimale cui le banche devono attenersi nell'orientare le proprie scelte in materia di controlli interni.

In particolare, le banche devono:

— verificare la coerenza dell'attività di ciascuna succursale o gruppo di succursali estere con gli obiettivi e le strategie aziendali;

— adottare procedure informative e contabili uniformi o comunque pienamente raccordabili con il sistema centrale, in modo da assicurare flussi informativi adeguati e tempestivi nei confronti degli organi aziendali;

— conferire poteri decisionali secondo criteri rapportati alle potenzialità delle succursali e attribuire le competenze tra le diverse unità operative di ciascuna succursale in modo da assicurare la necessaria dialettica nell'esercizio dell'attività;

— prevedere l'esercizio dei poteri di firma in forma congiunta; qualora le caratteristiche e la rischiosità delle operazioni lo richiedano, deve essere previsto l'intervento di dirigenti della succursale capo-area, ove esistente, o dell'organo con funzione di gestione. Eventuali deroghe per operazioni di importo e rischiosità limitati devono essere disciplinate con apposito regolamento;

— assoggettare le succursali estere ai controlli dell'*internal audit*, che devono essere effettuati da personale in possesso della necessaria specializzazione;

— istituire presso le succursali con una operatività significativa, tenuto conto sia della rischiosità della succursale rispetto alla complessiva propensione al rischio della banca, sia della complessità operativa/organizzativa della succursale stessa, un'unità incaricata dei controlli di secondo livello e un'unità avente funzioni di revisione interna. Gli addetti a tali unità, di norma gerarchicamente dipendenti dalle funzione aziendali di controllo centrali, riferiscono, oltre che ai responsabili di tali funzioni, attraverso specifiche relazioni direttamente al dirigente preposto alla succursale capo-area, ove esistente, e all'organo con funzione di gestione;

— effettuare il controllo documentale su tutti gli aspetti dell'operatività ed estenderlo anche al merito della gestione in modo da condurre a una valutazione complessiva dell'andamento delle succursali estere, sotto il profilo del reddito prodotto e dei rischi assunti; l'esito delle verifiche va sottoposto all'organo con funzione di gestione, che curerà, almeno una volta all'anno, uno specifico riferimento all'organo con funzione di supervisione strategica.

L'organo con funzione di gestione deve avere cura di intensificare, a fini di controllo sulla propria struttura periferica, i rapporti con le parallele strutture centrali delle principali banche corrispondenti, concordando tra l'altro idonee procedure per la verifica delle posizioni reciproche.

Nella selezione dei dirigenti da preporre alla guida delle filiali estere, gli organi aziendali devono tenere conto della capacità degli interessati di adeguarsi alla logica dell'organizzazione aziendale e alle regole di comportamento applicabili in generale alle banche italiane.

Vanno previste verifiche, la cui frequenza deve essere coerente con la tipologia di rischi assunti dalla succursale estera, da parte dell'organo con funzione di controllo, della funzione di revisione interna e delle società di revisione esterne. Le verifiche in loco condotte dalla funzione di revisione interna devono essere estese e riguardare almeno i rischi assunti, l'affidabilità delle strutture operative, i sistemi informativi, il funzionamento dei controlli interni, l'inserimento sul mercato. La periodicità minima delle verifiche è graduata in relazione all'operatività svolta e ai mercati di insediamento. I risultati delle verifiche sono portati tempestivamente a conoscenza degli organi aziendali.

ALLEGATO C

IL *RISK APPETITE FRAMEWORK*

1. Premessa.

Le banche definiscono un quadro di riferimento per la determinazione della propensione al rischio (*Risk Appetite Framework* - «RAF»), che fissi *ex ante* gli obiettivi di rischio/rendimento che l'intermediario intende raggiungere e i conseguenti limiti operativi.

La formalizzazione, attraverso la definizione del RAF, di obiettivi di rischio coerenti con il massimo rischio assumibile, il *business model* e gli indirizzi strategici è un elemento essenziale per la determinazione di una politica di governo dei rischi e di un processo di gestione dei rischi improntati ai principi della sana e prudente gestione aziendale.

Le banche, inoltre, coordinano il quadro di riferimento per la determinazione della propensione al rischio con il processo ICAAP (*cfr.* Titolo III, Capitolo 1) e ne assicurano la corretta attuazione attraverso una organizzazione e un sistema dei controlli interni adeguati.

2. Indicazioni sul contenuto del RAF.

Nel presente paragrafo sono fornite indicazioni minimali per la definizione del *Risk Appetite Framerwork*, fermo restando che l'effettiva articolazione del RAF va calibrata in base alle caratteristiche dimensionali e di complessità operativa di ciascuna banca.

Le banche assicurano una stretta coerenza e un puntuale raccordo tra: il modello di *business*, il piano strategico, il RAF (e i parametri utilizzati per definirlo), il processo ICAAP, i budget, l'organizzazione aziendale e il sistema dei controlli interni.

Il RAF, tenuto conto del piano strategico e dei rischi rilevanti ivi individuati, e definito il massimo rischio assumibile, indica le tipologie di rischio che la banca intende assumere; per ciascuna tipologia di rischio, fissa gli obiettivi di rischio, le eventuali soglie di tolleranza e i limiti operativi in condizioni sia di normale operatività, sia di stress. Sono, altresì, indicate le circostanze, inclusi gli esiti degli scenari di stress, al ricorrere delle quali l'assunzione di determinate categorie di rischio va evitata o contenuta rispetto agli obiettivi e ai limiti fissati.

Gli obiettivi di rischio, le soglie di tolleranza e i limiti di rischio sono, di norma, declinati in termini di:

a) misure espressive del capitale a rischio o capitale economico (VaR, *expected shortfall*, *ecc)*;

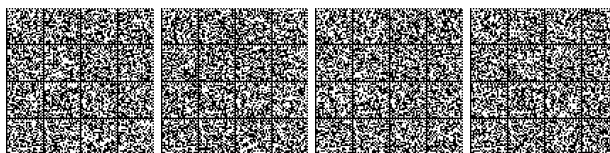
b) adeguatezza patrimoniale;

c) liquidità.

Con riferimento ai rischi quantificabili, la declinazione degli elementi costituenti del RAF avviene attraverso l'utilizzo di opportuni parametri quantitativi e qualitativi, calibrati in funzione del principio di proporzionalità; a tal fine, le banche possono fare riferimento alle metodologie di misurazione dei rischi utilizzate ai fini della valutazione aziendale dell'adeguatezza patrimoniale (ICAAP) (*cfr.* Titolo III, Capitolo 1, Sezione II).

Con riferimento ai rischi difficilmente quantificabili (quali, ad es, il rischio strategico, il rischio reputazionale o il rischio di *compliance*), il RAF fornisce specifiche indicazioni di carattere qualitativo che siano in grado di orientare la definizione e l'aggiornamento dei processi e dei presidi del sistema dei controlli interni.

Nel RAF sono definite le procedure e gli interventi gestionali da attivare nel caso in cui sia necessario ricondurre il livello di rischio entro l'obiettivo o i limiti prestabiliti. In particolare, sono definiti gli interventi gestionali da adottare al raggiungimento della soglia di tolleranza (ove definita). Sono precisate anche le tempistiche e le modalità da seguire per l'aggiornamento del RAF.

Il RAF, infine, precisa i compiti degli organi e di tutte le funzioni aziendali coinvolte nella definizione del processo.

TITOLO V

CAPITOLO 8
IL SISTEMA INFORMATIVO

Sezione I
DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa.

Il sistema informativo (inclusivo delle risorse tecnologiche — hardware, software, dati, documenti elettronici, reti telematiche — e delle risorse umane dedicate alla loro amministrazione) rappresenta uno strumento di primaria importanza per il conseguimento degli obiettivi strategici e operativi degli intermediari, in considerazione della criticità dei processi aziendali che dipendono da esso. Infatti:

— dal punto di vista strategico, un sistema informativo sicuro ed efficiente, basato su un'architettura flessibile, resiliente e integrata a livello di gruppo consente di sfruttare le opportunità offerte dalla tecnologia per ampliare e migliorare i prodotti e i servizi per la clientela, accrescere la qualità dei processi di lavoro, favorire la dematerializzazione dei valori, ridurre i costi anche attraverso la virtualizzazione dei servizi bancari;

— nell'ottica della sana e prudente gestione, il sistema informativo consente al *management* di disporre di informazioni dettagliate, pertinenti e aggiornate per l'assunzione di decisioni consapevoli e tempestive e per la corretta attuazione del processo di gestione dei rischi (*cfr.* Capitolo 7);

— con riguardo al contenimento del rischio operativo, il regolare svolgimento dei processi interni e dei servizi forniti alla clientela, l'integrità, la riservatezza e la disponibilità delle informazioni trattate, fanno affidamento sulla funzionalità dei processi e dei controlli automatizzati;

— in tema di *compliance*, al sistema informativo è affidato il compito di registrare, conservare e rappresentare correttamente i fatti di gestione e gli eventi rilevanti per le finalità previste da norme di legge e da regolamenti interni ed esterni.

Le previsioni contenute nel presente Capitolo rappresentano requisiti di carattere generale per lo sviluppo e la gestione del sistema informativo da parte degli intermediari; le concrete misure da adottare tengono conto degli specifici obiettivi strategici e, secondo il principio di proporzionalità, della dimensione e complessità operative, della natura dell'attività svolta, della tipologia dei servizi prestati nonché del livello di automazione dei processi e servizi della banca.

A tal proposito, le banche valutano l'opportunità di avvalersi degli standard e *best practices* definiti a livello internazionale in materia di governo, gestione, sicurezza e controllo del sistema informativo.

2. Fonti normative.

La materia è regolata:

— dalla direttiva del Parlamento europeo e del Consiglio 2013/36/UE del 26 giugno 2013, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE;

— dai seguenti articoli del TUB:

• art. 51, il quale prevede che le banche inviino alla Banca d'Italia, con le modalità e i tempi da essa stabiliti, le segnalazioni periodiche nonché ogni dato e documento richiesti;

• art. 53, comma 1, lett. *d)*, che attribuisce alla Banca d'Italia, in conformità delle delibere del CICR, il potere di emanare disposizioni di carattere generale in materia di organizzazione amministrativa e contabile e controlli interni delle banche;

• art. 67, comma 1, lett. *d)*, che attribuisce alla Banca d'Italia, in conformità delle delibere del CICR, il potere di impartire alla capogruppo di un gruppo bancario disposizioni concernenti il gruppo complessivamente considerato o i suoi componenti aventi ad oggetto l'organizzazione amministrativa e contabile e i controlli interni;

— dalla delibera del CICR del 2 agosto 1996, come modificata dalla delibera del 23 marzo 2004, in materia di organizzazione amministrativa e contabile e controlli interni delle banche e dei gruppi bancari;

— dal decreto del Ministro dell'Economia e delle finanze, Presidente del CICR del 5 agosto 2004 in materia, tra l'altro, di compiti e poteri degli organi sociali delle banche e dei gruppi bancari;

— dalle *Recommendations for the security of internet payments* emanate dalla BCE il 31 gennaio 2013 (32).

Si è anche tenuto conto del documento *Principles for effective risk data aggregation and risk reporting*, pubblicato dal Comitato di Basilea per la vigilanza bancaria nel gennaio 2013 (33).

3. Definizioni.

Ai fini della presente disciplina si definisce:

— «*accountability*»: l'assegnazione della responsabilità di un'attività o processo aziendale, con il conseguente compito di rispondere delle operazioni svolte e dei risultati conseguiti, a una determinata figura aziendale; in ambito tecnico, si intende la garanzia di poter attribuire ciascuna operazione a soggetti (utenti o applicazioni) univocamente identificabili;

— «*autenticazione*»: la procedura di verifica dell'identità di un utente da parte di un sistema o servizio;

— «*autorizzazione*»: la procedura che verifica se un cliente o un altro soggetto interno o esterno ha il diritto di compiere una certa azione, ad es. di trasferire fondi o accedere a dati sensibili;

— «*componente critica del sistema informativo*»: il sistema o l'applicazione per i quali un incidente di sicurezza informatica può pregiudicare il regolare e sicuro svolgimento di funzioni operative importanti (*cfr.* Capitolo 7, par. 3) per l'intermediario, tra cui l'efficace espletamento dei compiti degli organi aziendali e delle funzioni di controllo; l'analisi dei rischi definisce le funzioni aziendali e le componenti del sistema informativo che presentano rischi rilevanti per la banca;

— «*credenziali*»: le informazioni — generalmente riservate — utilizzate da un utente a fini di autenticazione ad un sistema o servizio. Sono inclusi nella definizione gli strumenti fisici che forniscono o memorizzano le informazioni (ad es., generatori di password non riutilizzabili, *smart card*) o qualcosa che l'utente ricorda (ad es., password) o rappresenta (ad es., caratteristiche biometriche);

— «*incidente di sicurezza informatica*»: ogni evento che implica la violazione o l'imminente minaccia di violazione delle norme e delle prassi aziendali in materia di sicurezza delle informazioni (ad es., frodi informatiche, attacchi attraverso internet e malfunzionamenti e disservizi);

— «*grave incidente di sicurezza informatica*»: un incidente di sicurezza informatica da cui derivi almeno una delle seguenti conseguenze:

a) perdite economiche elevate o prolungati disservizi per l'intermediario, anche a seguito di ripetuti incidenti di minore entità;

b) disservizi rilevanti sulla clientela e altri soggetti (ad es., intermediari o infrastrutture di pagamento); la valutazione della gravità considera il numero dei clienti o controparti potenzialmente coinvolti e l'ammontare a rischio;

c) il rischio di inficiare la capacità della banca di conformarsi alle condizioni e agli obblighi di legge o previsti dalla disciplina di vigilanza;

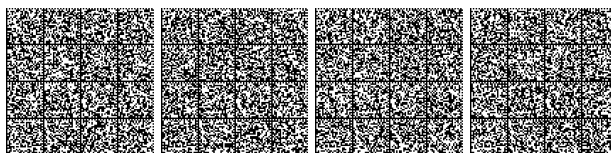
— «*minimo privilegio* (*least privilege*)»: il principio che stabilisce che a ciascun utente o amministratore di sistema siano assegnate le abilitazioni strettamente necessarie allo svolgimento dei compiti assegnati;

— «*no single point of failure*»: il principio architetturale secondo il quale l'eventuale guasto di un singolo componente di un sistema non compromette il regolare funzionamento dell'intero sistema;

— «*operazioni critiche*»: le operazioni relative a funzioni operative importanti effettuate in ambiente di produzione che, se errate o non effettuate, possono pregiudicare il regolare funzionamento di componenti critiche del sistema informativo (con riferimento a dati, a programmi o alla configurazione del sistema) nonché quelle che possono alterare, direttamente o indirettamente, i valori aziendali;

— «*procedura di contingency*»: una procedura che, in caso di indisponibilità o grave malfunzionamento del sistema, prevede il ricorso in condizioni di emergenza a strumenti a bassa integrazione nei processi

(32) http://www.ecb.europa.eu/pub/pdf/other/recommendationsforthesecurityofinternetpaymentsen.pdf.

(33) http://www.bis.org/publ/bcbs239.pdf

aziendali (ad es., ricorrendo ad attività manuali) al fine di completare un insieme limitato di operazioni di particolare criticità;

— «*procedura di fallback*»: una procedura attivata in occasione di gravi problemi in caso di aggiornamento tecnologico o migrazione a nuove piattaforme, volta a fornire modalità alternative per lo svolgimento delle funzioni applicative non funzionanti;

— «*rischio informatico* (*o ICT*)»: il rischio di incorrere in perdite economiche, di reputazione e di quote di mercato in relazione all'utilizzo di tecnologia dell'informazione e della comunicazione (*Information and Communication Technology - ICT*). Nella rappresentazione integrata dei rischi aziendali a fini prudenziali (ICAAP), tale tipologia di rischio è considerata, secondo gli specifici aspetti, tra i rischi operativi, reputazionali e strategici;

— «*rischio informatico residuo*»: il rischio informatico a cui l'intermediario è esposto una volta applicate le misure di attenuazione individuate nel processo di analisi dei rischi;

— «*risorsa informatica* (*o ICT*)»: un bene dell'azienda afferente all'ICT che concorre alla ricezione, archiviazione, elaborazione, trasmissione e fruizione dell'informazione gestita dall'intermediario;

— «*segregazione dei compiti* (*segregation of duties*)»: il principio che stabilisce che l'esecuzione di operazioni di particolare criticità sia svolta attraverso la cooperazione di più utenti o amministratori di sistema con responsabilità formalmente ripartite;

— «*utente responsabile*»: la figura aziendale identificata per ciascun sistema o applicazione e che ne assume formalmente la responsabilità, in rappresentanza degli utenti e nei rapporti con le funzioni preposte allo sviluppo e alla gestione tecnica;

— «*verificabilità*»: la garanzia di poter ricostruire, all'occorrenza e anche a distanza di tempo, eventi connessi all'utilizzo del sistema informativo e al trattamento di dati.

4. Destinatari della disciplina.

Le presenti disposizioni si applicano, secondo quanto stabilito nel Titolo I, Capitolo 1, Parte Seconda:

— alle banche autorizzate in Italia, ad eccezione delle succursali di banche extracomunitarie aventi sede nei paesi del Gruppo dei Dieci ovvero in quelli inclusi in un apposito elenco pubblicato e periodicamente aggiornato dalla Banca d'Italia (34);

— alle capogruppo di gruppi bancari;

— alle imprese di riferimento, secondo quanto previsto dalla Sezione VI del Capitolo 7.

Sezione II

GOVERNO E ORGANIZZAZIONE DEL SISTEMA INFORMATIVO

1. Premessa.

Nell'ambito della generale disciplina dell'organizzazione e dei controlli interni, sono attribuiti agli organi e funzioni aziendali ruoli e responsabilità, relativi allo sviluppo e alla gestione del sistema informativo, nel rispetto del principio della separazione delle funzioni di controllo da quelle di supervisione e gestione.

2. Compiti dell'organo con funzione di supervisione strategica.

L'organo con funzione di supervisione strategica assume la generale responsabilità di indirizzo e controllo del sistema informativo, nell'ottica di un ottimale impiego delle risorse tecnologiche a sostegno delle strategie aziendali (*ICT governance*). In tale ambito esso:

— approva le strategie di sviluppo del sistema informativo, in considerazione dell'evoluzione del settore di riferimento e in coerenza con l'articolazione in essere e a tendere dei settori di operatività, dei processi e dell'organizzazione aziendale; in tale contesto approva il modello di riferimento per l'architettura del sistema informativo;

(34) Alle banche che prestano attività e servizi di investimento si applicano anche le disposizioni contenute nel Regolamento della Banca d'Italia e della Consob del 29 ottobre 2007, come successivamente modificato e integrato, in materia di organizzazione e procedure degli intermediari che prestano servizi di investimento o di gestione collettiva del risparmio.

— approva la *policy* di sicurezza informatica (35);

— approva le linee di indirizzo in materia di selezione del personale con funzioni tecniche e di acquisizione di sistemi, software e servizi, incluso il ricorso a fornitori esterni (*cfr.* Sezione VI);

— promuove lo sviluppo, la condivisione e l'aggiornamento di conoscenze in materia di ICT all'interno dell'azienda;

— è informato con cadenza almeno annuale circa l'adeguatezza dei servizi erogati e il supporto di tali servizi all'evoluzione dell'operatività aziendale, in rapporto ai costi sostenuti; è informato tempestivamente in caso di gravi problemi per l'attività aziendale derivanti da incidenti e malfunzionamenti del sistema informativo.

Con specifico riguardo all'esercizio della responsabilità di supervisione della analisi del rischio informatico (*cfr.* Sezione III), lo stesso organo:

— approva il quadro di riferimento organizzativo e metodologico per l'analisi del rischio informatico, promuovendo l'opportuna valorizzazione dell'informazione sul rischio tecnologico all'interno della funzione ICT e l'integrazione con i sistemi di misurazione e gestione dei rischi (in particolare quelli operativi, reputazionali e strategici);

— approva la propensione al rischio informatico, avuto riguardo ai servizi interni e a quelli offerti alla clientela, in conformità con gli obiettivi di rischio e il quadro di riferimento per la determinazione della propensione al rischio definiti a livello aziendale (*cfr.* Capitolo 7, Allegato C);

— è informato con cadenza almeno annuale sulla situazione di rischio informatico rispetto alla propensione al rischio.

Nell'Allegato A, sono riportati i documenti che l'organo con funzione di supervisione strategica approva nell'ambito del suo ruolo e responsabilità nella materia.

3. Compiti dell'organo con funzione di gestione.

L'organo con funzione di gestione ha il compito di assicurare la completezza, l'adeguatezza, la funzionalità (in termini di efficacia ed efficienza) e l'affidabilità del sistema informativo. In particolare, tale organo:

— definisce la struttura organizzativa della funzione ICT (ove presente) (36) assicurandone nel tempo la rispondenza alle strategie e ai modelli architetturali definiti dall'organo con funzione di supervisione strategica; garantisce il corretto dimensionamento quali-quantitativo delle risorse umane;

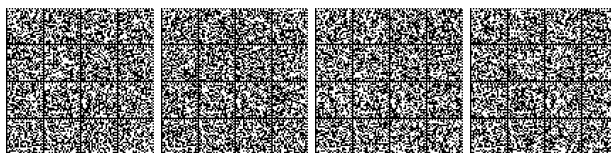
— definisce l'assetto organizzativo, metodologico e procedurale per il processo di analisi del rischio informatico, perseguendo un opportuno livello di raccordo con la funzione di *risk management* per i processi di stima del rischio operativo;

— tranne che nel caso di *full outsourcing*, approva il disegno dei processi di gestione del sistema informativo, garantendo l'efficacia ed efficienza dell'impianto nonché la complessiva completezza e coerenza, con particolare riguardo ad una funzionale assegnazione di compiti e responsabilità, alla robustezza dei controlli, alla validità del supporto metodologico e procedurale;

— approva gli standard di *data governance*, le procedure di gestione dei cambiamenti e degli incidenti (ove del caso, in raccordo con le procedure del fornitore di servizi) e, di norma con cadenza annuale, il piano operativo delle iniziative informatiche, verificandone la coerenza con le esigenze informative e di automazione delle linee di *business* nonché con le strategie aziendali;

— valuta almeno annualmente le prestazioni della funzione ICT rispetto alle strategie e agli obiettivi fissati, in termini di rapporto costi /

(35) Nel caso di full outsourcing del sistema informativo l'organo di supervisione strategica, qualora non abbia le necessarie competenze al proprio interno, potrà avvalersi di risorse esterne indipendenti dal fornitore di servizi. Inoltre, nella definizione dei documenti richiesti (cfr. Allegato A), si può fare riferimento ad analoga documentazione prodotta dal fornitore.

(36) Nel caso di gruppo bancario che abbia accentrato la funzione ICT in una società controllata del gruppo, il compito di definizione della funzione ICT può essere demandato all'organo con funzione di gestione di tale società, previa individuazione di opportuni canali informativi verso gli organi aziendali della capogruppo.

benefici o utilizzando sistemi integrati di misurazione delle prestazioni (37), assumendo gli opportuni interventi e iniziative di miglioramento;

— approva almeno annualmente la valutazione del rischio delle componenti critiche nonché la relazione sull'adeguatezza e costi dei servizi ICT, informando a tale riguardo l'organo con funzione di supervisione strategica; in tale ambito, riscontra la complessiva situazione del rischio informatico in rapporto alla propensione al rischio definita, disponendo allo scopo di idonei flussi informativi concernenti, come minimo, il livello di rischio residuo per le diverse risorse informatiche, lo stato di implementazione dei presidi di attenuazione del rischio (*cfr.* Sezione III), l'evoluzione delle minacce connesse con l'utilizzo di ICT nonché gli incidenti registratisi nel periodo di riferimento;

— monitora il regolare svolgimento dei processi di gestione e di controllo dei servizi ICT e, a fronte di anomalie rilevate, pone in atto opportune azioni correttive;

— assume decisioni tempestive in merito a gravi incidenti di sicurezza informatica (*cfr.* Sezione IV) e fornisce informazioni all'organo con funzione di supervisione strategica in caso di gravi problemi per l'attività aziendale derivanti da incidenti e malfunzionamenti.

In relazione alla responsabilità e ai compiti assegnati, l'organo con funzione di gestione è dotato di competenze tecnico-manageriali, tenuto conto della dimensione, complessità e articolazione organizzativa dell'intermediario nonché delle strategie di *sourcing*.

Nell'Allegato A sono riportati le procedure, gli standard e i piani soggetti all'approvazione dell'organo con funzione di gestione.

4. Organizzazione della funzione ICT.

L'articolazione organizzativa della funzione ICT dipende da fattori quali la complessità della struttura societaria, la dimensione, i settori di attività, le strategie di *business* e gestionali. Essa si ispira a criteri di funzionalità, efficienza e sicurezza, definendo chiaramente compiti e responsabilità e contemplando in particolare:

— linee di riporto dirette a livello dell'organo con funzione di gestione (38) a garanzia dell'unitarietà della visione gestionale e del rischio informatico nonché dell'uniformità di applicazione delle norme riguardanti il sistema informativo; eventuali unità di sviluppo decentrato sotto il controllo delle linee di *business* sono comunque inquadrate nel più generale disegno architetturale e agiscono nell'ambito di regole definite a livello aziendale;

— le responsabilità e gli assetti connessi con la pianificazione e il controllo del portafoglio dei progetti informatici, con il governo dell'evoluzione dell'architettura e dell'innovazione tecnologica nonché con le attività di gestione del sistema informativo (39);

— la realizzazione degli opportuni meccanismi di raccordo con le linee di *business*, con particolare riguardo alle attività di individuazione e pianificazione delle iniziative informatiche (regolare rilevazione delle esigenze di servizi informatici e promozione delle opportunità tecnologiche offerte dall'evoluzione del sistema informativo).

(37) I sistemi integrati di misurazione e reporting delle prestazioni sono procedure automatizzate, di norma basate su metodologie (ad es., balanced scorecards) volte a tracciare un profilo integrato del complessivo andamento dell'azienda o di una specifica funzione aziendale, attraverso il ricorso ad indicatori di prestazione (KPI - key performance indicators) e valori di riferimento (benchmark) opportunamente individuati. In caso di outsourcing è opportuno definire nel contratto un insieme di report minimi, utili anche a verificare il rispetto delle SLA (Service level agreement).

(38) Nel caso di gruppo bancario che abbia accentrato la funzione ICT in una società controllata, è possibile individuare all'interno di questa l'organo responsabile di tale funzione per l'intero gruppo, purché siano stabiliti canali informativi diretti tra esso e l'organo con funzione di gestione della capogruppo; in tale opzione, l'organo con funzione di gestione della capogruppo assume la responsabilità di seguire la pianificazione delle iniziative ICT, garantendone la rispondenza alle esigenze e alle strategie del gruppo.

(39) Nel caso di full outsourcing della funzione ICT, al «referente per l'attività esternalizzata» (cfr. Capitolo 7, Sezione IV, par. 1) è assegnata la responsabilità di seguire la pianificazione dei progetti informatici; la stessa figura garantisce, in collaborazione con il fornitore di servizi, la realizzazione degli opportuni meccanismi di raccordo con le linee di business.

5. La sicurezza informatica.

La funzione di sicurezza informatica è deputata allo svolgimento dei compiti specialistici in materia di sicurezza delle risorse ICT. In particolare:

— segue la redazione e l'aggiornamento delle *policy* di sicurezza e delle istruzioni operative;

— assicura la coerenza dei presidi di sicurezza con le *policy* approvate;

— partecipa alla progettazione, realizzazione e manutenzione dei presidi di sicurezza dei *data center*;

— partecipa alla valutazione del rischio potenziale nonché all'individuazione dei presidi di sicurezza nell'ambito del processo di analisi del rischio informatico (*cfr.* Sezione III);

— assicura il monitoraggio nel continuo delle minacce applicabili alle diverse risorse informatiche (*cfr.* Sezione IV, par. 3);

— segue lo svolgimento dei test di sicurezza prima dell'avvio in produzione di un sistema nuovo o modificato (*cfr.* Sezione IV, par. 5).

Nelle realtà più complesse, l'indipendenza di giudizio rispetto alle funzioni operative è assicurata da un'adeguata collocazione organizzativa.

6. Il controllo del rischio informatico e la *compliance* ICT.

Nell'ambito del sistema dei controlli interni sono chiaramente assegnate responsabilità in merito allo svolgimento dei seguenti compiti di controllo di secondo livello:

— il controllo dei rischi, basato su flussi informativi continui in merito all'evoluzione del rischio informatico e sul monitoraggio dell'efficacia delle misure di protezione delle risorse ICT. La gestione del complessivo rischio informatico si raccorda con il processo di analisi sulle singole risorse ICT (*cfr.* Sezione III). Le valutazioni svolte sono documentate e riviste in rapporto ai risultati del monitoraggio e comunque almeno una volta l'anno.

Con riferimento alle banche con un modello interno validato sul rischio operativo, i dati sulle perdite operative in ambito ICT sono integrati con i dati e gli scenari relativi alle altre funzioni aziendali, e ne sono presidiati la qualità e completezza;

— il rispetto dei regolamenti interni e delle normative esterne in tema di ICT (ICT *compliance*) garantendo, tra l'altro:

• l'assistenza su aspetti tecnici in caso di questioni legali relative al trattamento dei dati personali;

• la coerenza degli assetti organizzativi alle normative esterne, per le parti relative al sistema informativo;

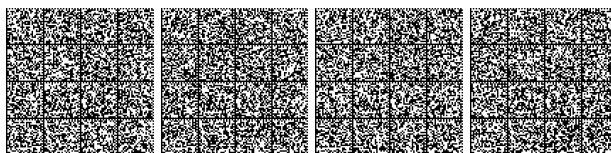
• l'analisi di conformità dei contratti di *outsourcing* e con fornitori (inclusi i contratti infra-gruppo).

7. Compiti della funzione di revisione interna.

L'*internal audit* dispone — al suo interno o mediante il ricorso a risorse esterne (40) — delle competenze specialistiche necessarie per assolvere ai propri compiti di assurance attinenti al sistema informativo aziendale (ICT *audit*).

La pianificazione degli interventi ispettivi assicura nel tempo un'adeguata copertura delle varie applicazioni, infrastrutture e processi di gestione, incluse le eventuali componenti esternalizzate (41). A prescindere dalla forma adottata per gli accertamenti (ad es., *audit* mirati ovvero verifiche sulle applicazioni e componenti del sistema informativo nell'ambito di ispezioni su strutture organizzative o processi produttivi), l'*internal audit* è in grado di fornire valutazioni sui principali rischi tecnologici identificabili e sulla complessiva gestione del rischio informatico dell'intermediario.

(40) Anche in caso di ricorso all'esterno, le risorse impegnate nell'audit mantengono l'indipendenza rispetto alle unità assoggettate al controllo.

(41) Tenuto conto del principio di proporzionalità, per le verifiche su componenti o servizi ICT esternalizzati, la funzione di audit dell'intermediario potrà scegliere, sotto la sua responsabilità, di fare affidamento sull'internal audit del fornitore di servizi, previa valutazione della sua professionalità e indipendenza.

Sezione III
L'ANALISI DEL RISCHIO INFORMATICO

L'analisi del rischio informatico costituisce uno strumento a garanzia dell'efficacia ed efficienza delle misure di protezione delle risorse ICT, permettendo di graduare le misure di mitigazione nei vari ambienti in funzione del profilo di rischio dell'intermediario.

Il processo di analisi è svolto con il concorso dell'utente responsabile (42), del personale della funzione ICT, delle funzioni di controllo dei rischi, di sicurezza informatica e, ove opportuno, dell'*audit*, secondo metodologie e responsabilità formalmente definite dall'organo con funzione di gestione. Esso si compone delle seguenti fasi:

— la valutazione del rischio potenziale cui sono esposte le risorse informatiche esaminate; tale attività interessa tutte le iniziative di sviluppo di nuovi progetti e di modifica rilevante del sistema informativo (43).

Tale fase prende l'avvio con la classificazione delle risorse ICT (44) in termini di rischio informatico (45);

— il trattamento del rischio, volto a individuare, se necessario, misure di attenuazione — di tipo tecnico o organizzativo — idonee a contenere il rischio potenziale.

L'analisi determina il rischio residuo da sottoporre ad accettazione formale dell'utente responsabile (46). Qualora il rischio residuo ecceda la propensione al rischio informatico, approvato dall'organo con funzione di supervisione strategica (*cfr.* Sezione II, par. 2), l'analisi propone l'adozione di misure alternative o ulteriori di trattamento del rischio (47), definite con il coinvolgimento della funzione di controllo dei rischi e sottoposte all'approvazione dell'organo con funzione di gestione.

Per le procedure in esercizio, per le quali non è stata svolta un'analisi del rischio in fase di sviluppo, è comunque prevista una valutazione integrativa, al fine di individuare eventuali presidi in aggiunta a quelli già in essere, da attuare secondo uno specifico piano di implementazione. I tempi di attuazione del piano e i presidi compensativi di tipo organizzativo o procedurale nelle more dell'attuazione, sono documentati e sottoposti all'accettazione formale dell'utente responsabile.

I risultati del processo (livelli di classificazione, rischi potenziali e residui, lista delle minacce considerate, elenco dei presidi individuati), ogni loro aggiornamento successivo, le assunzioni operate e le decisioni assunte, sono documentati e portati a conoscenza dell'organo con funzione di gestione.

Il processo di analisi del rischio è ripetuto con periodicità adeguata alla tipologia delle risorse ICT e dei rischi e, comunque, in presenza di situazioni che possono influenzare il complessivo livello di rischio informatico (48).

Sezione IV
LA GESTIONE DELLA SICUREZZA INFORMATICA

1. Premessa.

La gestione della sicurezza informatica comprende i processi e le misure volti, in raccordo con la generale azione aziendale per preservare la sicurezza delle informazioni e dei beni aziendali, a garantire a ciascuna risorsa informatica una protezione, in termini di riservatezza, integrità, disponibilità, verificabilità e *accountability*, appropriata e coerente lungo l'intero ciclo di vita.

Obiettivo di tale processo è anche di contribuire alla conformità del sistema informativo alle norme di legge e a regolamenti interni ed esterni.

La struttura dei processi e l'intensità dei presidi da porre in atto dipende dalle risultanze del processo di analisi dei rischi (*cfr.* Sezione III).

2. *Policy* di sicurezza.

La *policy* di sicurezza informatica è approvata dall'organo con funzione di supervisione strategica e comunicata a tutto il personale e alle terze parti coinvolte nella gestione di informazioni e componenti del sistema informativo. Essa riporta:

— gli obiettivi del processo di gestione della sicurezza informatica in linea con la propensione al rischio informatico definito a livello aziendale (*cfr.* Sezione II, par. 2); tali obiettivi sono espressi in termini di esigenze di protezione e di controllo del rischio tecnologico;

— i principi generali di sicurezza sull'utilizzo e la gestione del sistema informativo da parte dei diversi profili aziendali;

— i ruoli e le responsabilità connessi alla funzione di sicurezza informatica nonché all'aggiornamento e verifica delle *policy*;

— il quadro di riferimento organizzativo e metodologico dei processi di gestione dell'ICT deputati a garantire l'appropriato livello di protezione;

— le linee di indirizzo per le attività di comunicazione, formazione e sensibilizzazione delle diverse classi di utenti;

— un richiamo alle norme interne che disciplinano le conseguenze di violazioni rilevate della *policy* da parte del personale;

— un richiamo alle norme di legge e alle altre normative esterne applicabili inerenti alla sicurezza di informazioni e risorse ICT, incluse le norme riportate nella presente Sezione.

La *policy* di sicurezza può fare riferimento a documenti di maggiore dettaglio, ad es. linee guida o manuali operativi in tema di configurazioni e procedure di sicurezza per particolari componenti e applicazioni; *policy* dedicata per i servizi di pagamento via internet; norme per il corretto utilizzo di applicazioni aziendali trasversali, quali la posta elettronica e la navigazione internet.

La regolare revisione della *policy* di sicurezza tiene conto dell'evoluzione del campo di attività, dei prodotti forniti, delle tecnologie e dei rischi fronteggiati dall'intermediario (*cfr.* Sezione III).

3. La sicurezza delle informazioni e delle risorse ICT.

La sicurezza delle informazioni e delle risorse informatiche è garantita attraverso misure di protezione a livello fisico e logico, la cui intensità di applicazione è graduata in relazione alle risultanze della valutazione del rischio (classificazione delle risorse informatiche in termini di sicurezza). Tali misure sono distribuite su diversi strati, così che un'eventuale falla in una linea di difesa sia coperta dalla successiva («difesa in profondità»), comprendendo:

— i presidi fisici di difesa e le procedure di autorizzazione e controllo per l'accesso fisico a sistemi e dati (ad es., barriere perimetrali con punti di ingresso vigilati, locali ad accesso controllato con registrazione degli ingressi e delle uscite);

---

(42) Per le componenti e applicazioni critiche l'utente responsabile è individuato a un adeguato livello gerarchico. In caso di esternalizzazione del sistema, il referente per l'attività esternalizzata (cfr. Capitolo 7, Sezione IV, par. 1) partecipa, in qualità di utente responsabile, all'analisi del rischio svolta dal fornitore di servizi, anche tramite «comitati utente»; nel caso di full outsourcing presso una società strumentale del gruppo di appartenenza, l'utente responsabile è collocato all'esterno della funzione ICT (ad es., presso la capogruppo, secondo un modello accentrato, o presso i singoli intermediari, nell'approccio decentrato).

(43) In sede di valutazione dei rischi su componenti del sistema informativo e applicazioni già in essere, la banca tiene conto dei dati disponibili in merito agli incidenti di sicurezza informatica verificatisi in passato (cfr. Sezione IV, par. 6).

(44) La classificazione delle informazioni gestite mediante strumenti ICT è opportunamente raccordata con il trattamento delle informazioni aziendali in formato diverso da quello elettronico, onde conseguire uniformi livelli di protezione indipendentemente dalle modalità di trattamento.

(45) Ad esempio, con riferimento alla sicurezza informatica, va assegnato un indicatore di criticità in relazione al potenziale impatto di eventuali violazioni dei livelli di riservatezza, integrità, disponibilità richiesti dall'utente responsabile e alla probabilità di accadimento delle minacce che potrebbero causare tali violazioni.

(46) Nel documento approvato dall'utente responsabile, il rischio residuo è chiaramente espresso, perlomeno in termini qualitativi e con una descrizione non tecnica degli eventi dannosi che potrebbero comunque verificarsi in determinate circostanze.

(47) Ad esempio, si potrebbe ritenere di non abilitare funzioni o operazioni troppo rischiose (risk avoidance), ovvero di acquisire una polizza assicurativa (risk transfer).

(48) Tra le situazioni suscettibili di modificare gli scenari di rischio e il livello di rischio informatico valutato — e che quindi richiedono la revisione dell'analisi del rischio — ci sono il verificarsi di gravi incidenti, la rilevazione di carenze nei controlli, la diffusione di notizie su nuove vulnerabilità o minacce.

— la regolamentazione dell'accesso logico a reti, sistemi, basi di dati sulla base delle effettive esigenze operative (principio del *need to know*); i diritti di accesso sono accordati, mediante ricorso ad opportuni profili abilitativi, previa formale autorizzazione; l'elenco degli utenti abilitati è sottoposto a verifica con periodicità definita;

— la procedura di autenticazione per l'accesso alle applicazioni e ai sistemi; in particolare sono garantiti l'univoca associazione a ciascun utente delle proprie credenziali di accesso, il presidio della riservatezza dei fattori di autenticazione (49), l'osservanza degli standard definiti all'interno nonché delle normative applicabili, ad es. in materia di composizione e gestione della password, di limiti ai tentativi di accesso, di lunghezza di chiavi crittografiche;

— la segmentazione della rete di telecomunicazione, con controllo dei flussi scambiati, in particolare tra domini connotati da diversi livelli di sicurezza (ad es., sistemi e utenti interni, applicazioni *core*, sistemi e utenti esterni); l'accesso a sistemi e servizi critici tramite canali pubblici (ad es., nel caso dell'*e-banking* tramite internet) sono presidiati in modo da soddisfare rigorosi requisiti di sicurezza e fornire un livello di protezione conforme ai rischi da fronteggiare (50);

— l'adozione di metodologie e tecniche per lo sviluppo sicuro del software quale possibile presidio di difesa per componenti valutate nell'analisi del rischio informatico a un livello di rischio potenziale elevato;

— la separazione degli ambienti di sviluppo, collaudo e produzione, con adeguata formalizzazione del passaggio di moduli software tra di essi (par. 5), al fine di evitare — di norma — l'accesso a dati riservati e componenti critiche da parte del personale addetto allo sviluppo (51); l'ambiente di produzione è sottoposto a misure più restrittive di controllo degli accessi e delle modifiche;

— i criteri per la selezione e la gestione del personale adibito al trattamento dei dati e allo svolgimento di operazioni critiche (amministratori di sistema e utenti privilegiati) con particolare riguardo alla valutazione delle competenze e dell'affidabilità del personale, alla stipula di specifici impegni di riservatezza nonché alla gestione nel continuo delle mansioni assegnate (ad es., per mezzo di verifiche periodiche degli elenchi del personale abilitato e di misure di *job rotation*);

— le procedure per lo svolgimento delle operazioni critiche, garantendo il rispetto dei principi del minimo privilegio e della segregazione dei compiti (ad es., specifiche procedure di abilitazione e di autenticazione, controlli di tipo *four eyes* (52), o di verifica giornaliera *ex post*);

— il monitoraggio, anche attraverso l'analisi di log e tracce di *audit*, di accessi, operazioni e altri eventi al fine di prevenire e gestire gli incidenti di sicurezza informatica; le attività degli amministratori di sistema e altri utenti privilegiati delle componenti critiche sono sottoposte a stretto controllo;

— il monitoraggio continuativo delle minacce e delle vulnerabilità di sicurezza;

— le regole di tracciabilità delle azioni svolte, finalizzate a consentire la verifica a posteriori delle operazioni critiche, con l'archiviazione dell'autore, data e ora (53), contesto operativo e altre caratteristiche salienti della transazione. Le tracce elettroniche sono conservate per un periodo non inferiore a 24 mesi in archivi non modificabili o le cui modifiche sono puntualmente registrate.

(49) La procedura di generazione e di gestione fattori delle credenziali di autenticazione (ad es., password, smart card, token) garantisce che essi siano unici e nella disponibilità esclusiva del legittimo utente assegnatario, fatta salva la possibilità di definire procedure sicure per permettere all'intermediario di accedere a dati aziendali in caso di necessità, in assenza degli utenti abilitati.

(50) Con riferimento ai servizi di pagamento tramite internet si applicano le già citate Recommendations for the security of internet payments. emanate dalla BCE (http://www.ecb.europa.eu/pub/pdf/other/recommendationsforthesecurityofinternetpaymentsen.pdf).

(51) Tale accesso può essere concesso agli sviluppatori in casi specificamente disciplinati, in via temporanea e previa autorizzazione dell'utente responsabile.

(52) Si fa riferimento a controlli applicativi che richiedono l'inserimento di una stessa transazione da parte di due diversi utenti per procedere alla sua esecuzione.

(53) Ai fini della possibilità di una corretta e agevole ricostruzione di eventi e operazioni che coinvolgono più sistemi, inclusi eventualmente sistemi esterni, è opportuno che l'intermediario si doti di un sistema unificato di riferimento temporale, ad es. basato sul protocollo standard NTP e sincronizzato con un segnale orario di riferimento ufficiale.

4. La sicurezza delle applicazioni sviluppate dalle unità operative e di controllo.

Lo sviluppo di applicazioni direttamente in carico alle unità operative e di controllo è sottoposto a misure di natura organizzativa e metodologica, tese a garantire un livello di sicurezza comparabile con le applicazioni sviluppate dalla funzione ICT.

Un periodico monitoraggio censisce le applicazioni sviluppate con strumenti di informatica d'utente e ne verifica la rispondenza alla *policy* di sicurezza, in particolare se utilizzate in attività rilevanti quali la predisposizione dei dati di bilancio, del *risk management*, della finanza e del *reporting* direzionale, al fine di contenere il rischio operativo (54).

5. La gestione dei cambiamenti.

La procedura di gestione dei cambiamenti delle applicazioni e risorse ICT è formalmente definita e garantisce il controllo su modifiche, sostituzioni o adeguamenti tecnologici, in particolare nell'ambiente di produzione. Il processo si svolge sotto la responsabilità di una figura o struttura aziendale con elevato grado di indipendenza rispetto alla funzione di sviluppo e prevede, in modo proporzionato alla complessità e al profilo di rischio tecnologico dell'intermediario:

— la predisposizione e il costante aggiornamento nel tempo di un inventario o mappa del patrimonio ICT (hardware, software, dati, procedure) (55);

— la valutazione dell'impatto dei cambiamenti sul sistema e dei rischi correlati con le proposte di modifica;

— l'autorizzazione formale di ogni cambiamento in ambiente di produzione (56); tale procedura comprende l'accettazione, nei casi critici individuati nell'analisi dei rischi, nel nuovo rischio residuo;

— la pianificazione, il coordinamento e la documentazione degli interventi di modifica, prevedendo attività di collaudo e test di sicurezza, in un ambiente deputato e distinto da quello di produzione;

— il ricorso a un idoneo sistema di gestione della configurazione di sistema (hardware, software, procedure di gestione e utilizzo, modalità di interconnessione), per il controllo dell'implementazione dei cambiamenti, inclusa la possibilità di ripristino della situazione *ex ante*.

Le modifiche in caso di emergenza possono essere gestite con presidi non pienamente conformi alle *policy* ordinarie ma comunque adeguati alla particolare situazione. Tali modifiche sono comunque sottoposte a tracciamento e notificate *ex post* all'utente responsabile.

Le iniziative di ampio impatto sul sistema informativo (ad es., modifiche rilevanti sulle componenti critiche, adeguamenti in conseguenza di fusioni o scissioni, migrazione ad altre piattaforme informatiche) — che si inseriscono di norma in piani strategici all'attenzione dell'organo con funzione di supervisione strategica — sono preventivamente comunicate alla Banca d'Italia e prevedono, in aggiunta a quanto sopra specificato, idonee misure, tecniche, organizzative e procedurali, volte a garantire un avvio in esercizio controllato e con limitati impatti sui servizi forniti alla clientela (ad es., implementazione per stadi successivi, periodi di esercizio in parallelo con la precedente procedura, procedure di *fallback* e *contingency*). Flussi informativi verso i vari livelli manageriali e gli organi aziendali consentono il monitoraggio dell'avanzamento del progetto.

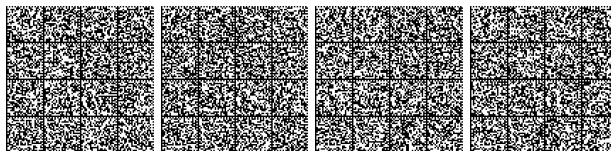
6. La gestione degli incidenti di sicurezza informatica.

La gestione degli incidenti di sicurezza informatica segue procedure formalmente definite, con l'obiettivo di minimizzare l'impatto di eventi avversi e garantire il tempestivo ripristino del regolare funzionamento dei servizi e delle risorse ICT coinvolti. Le funzioni a cui comunicare l'incidente sono individuate secondo un'opportuna procedura di *escalation*; i casi più gravi che comportino rischi di interruzione della continuità operativa sono segnalati alla struttura preposta a dichiarare lo stato di crisi (*cfr.* Capitolo 9).

A seguito dell'analisi degli incidenti di sicurezza informatica e dei relativi rilievi delle funzioni di *audit* e della *compliance* sono definite e monitorate le azioni correttive.

(54) Tale censimento è anche utile a verificare il grado di copertura delle esigenze garantito dalle procedure messe a disposizione dalla funzione ICT.

(55) L'inventario aggiornato del sistema e delle risorse ICT è funzionale anche alle attività di analisi del rischio informatico (cfr. Sezione III).

(56) Il livello autorizzativo è adeguato all'entità dei rischi emersi nell'analisi.

In ogni caso, le informazioni salienti dell'evento e i passi seguiti nella gestione dello stesso sono documentati.

Il processo si raccorda con il monitoraggio di sistemi, accessi e operazioni (*cfr.* par. 3) nonché con la gestione dei malfunzionamenti e delle segnalazioni di problemi da parte degli utenti interni ed esterni, favorendo l'assunzione di iniziative di prevenzione (57).

Le procedure definite per gravi incidenti di sicurezza informatica includono la cooperazione con le forze dell'ordine preposte e con gli altri operatori o enti coinvolti, anche in caso di fuoriuscite di informazioni.

I gravi incidenti di sicurezza informatica sono comunicati tempestivamente alla Banca d'Italia, con l'invio di un rapporto sintetico recante una descrizione dell'incidente e dei disservizi provocati agli utenti interni e alla clientela nonché i seguenti dati, accertati o presunti: *i)* data e ora dell'accadimento o della manifestazione dell'incidente; *ii)* risorse e servizi coinvolti; *iii)* cause, tempi e modalità previsti per il pieno ripristino dei livelli di disponibilità e sicurezza definiti e per il completo accertamento dei fatti connessi; *iv)* descrizione delle azioni intraprese e dei risultati ottenuti; *v)* una valutazione dei danni delle perdite economiche o danni d'immagine.

7. La disponibilità delle informazioni e delle risorse ICT.

La disponibilità dell'accesso a dati e dei servizi telematici è garantita agli utenti autorizzati in orari e con modalità conformi alle esigenze (58). A tal fine, i processi interessati (definizione dei modelli architetturali, sviluppo di applicazioni e infrastrutture, gestione dei problemi tecnici, monitoraggio e pianificazione della capacità elaborativa e trasmissiva, gestione dei fornitori) tengono conto delle seguenti indicazioni:

— con riguardo alle applicazioni di maggiore criticità e ai servizi ICT rivolti alla clientela sono formalmente definiti i livelli di servizio che l'intermediario si impegna ad osservare; le prestazioni delle componenti critiche rispetto a tali livelli sono regolarmente monitorate e formano oggetto di sintetici rapporti disponibili periodicamente a tutte le parti interessate; è assicurata la congruità tra i livelli di servizio definiti per le componenti tra loro dipendenti;

— in relazione alle esigenze di disponibilità delle singole applicazioni, sono definite procedure di *backup* (di dati, software e configurazione) e di ripristino su sistemi alternativi, in precedenza individuati;

— le architetture sono disegnate in considerazione dei profili di sicurezza informatica delle applicazioni ospitate, tenendo conto di tutte le risorse ICT e di supporto interessate (alimentazione elettrica, impianti di condizionamento, ecc.); a tale riguardo, l'intermediario valuta la necessità di predisporre piattaforme particolarmente robuste e ridondate (ad es., applicando il principio del *no single point of failure*) volte a garantire l'alta disponibilità delle applicazioni maggiormente critiche, in sinergia con le procedure e il sistema di *disaster recovery*;

— in funzione dei profili di rischio delle comunicazioni, delle applicazioni e dei servizi acceduti, i collegamenti telematici interni alla banca o al gruppo sono opportunamente ridondati; in relazione al rischio di incidenti di sicurezza informatica che possono determinare l'interruzione dei servizi (ad es., mediante attacchi di tipo *denial of service o distributed denial of service*), oltre a soluzioni specifiche per l'individuazione e il blocco del traffico malevolo, la banca valuta l'opportunità di sfruttare procedure e strumenti per l'allocazione dinamica di capacità trasmissiva ed elaborativa;

— la gestione del sistema informativo è opportunamente automatizzata e si avvale, per quanto possibile, di procedure standardizzate; le operazioni di manutenzione ordinaria e straordinaria sono pianificate e comunicate con congruo anticipo agli utenti interessati;

— le informazioni raccolte attraverso il processo di monitoraggio delle risorse ICT alimentano il regolare processo di *capacity planning* (59) e sono utilizzate nella progettazione dell'evoluzione del sistema informativo.

(57) Nel caso delle banche AMA il processo è integrato con la rilevazione delle perdite operative.

(58) Si tiene conto del profilo di utilizzo (noto o stimato) nell'arco del calendario e per l'orario di operatività, con particolare attenzione a eventuali picchi elaborativi.

(59) Si intende per capacity planning il processo di gestione dell'ICT volto a stimare la quantità di risorse informatiche necessarie a fronteggiare le esigenze delle applicazioni aziendali nell'arco di un determinato periodo futuro.

Sezione V

IL SISTEMA DI GESTIONE DEI DATI

Il sistema di registrazione e *reporting* dei dati è deputato a tracciare tempestivamente tutte le operazioni aziendali e i fatti di gestione al fine di fornire informazioni complete e aggiornate sulla attività aziendali e sull'evoluzione dei rischi. Esso assicura nel continuo l'integrità, completezza e correttezza dei dati conservati e delle informazioni rappresentate; inoltre, garantisce l'*accountability* e l'agevole verificabilità (ad es., da parte delle funzioni di controllo) delle operazioni registrate.

In particolare, il sistema di gestione dei dati soddisfa i seguenti requisiti:

— la registrazione dei fatti aziendali è completa, corretta e tempestiva, al fine di consentire la ricostruzione dell'attività svolta (60);

— è definito uno standard aziendale di *data governance*, che individua ruoli e responsabilità delle funzioni coinvolte nell'utilizzo e nel trattamento, a fini operativi e gestionali delle informazioni aziendali (61); in considerazione della loro rilevanza nel sistema informativo, sono definite le misure atte a garantire e a misurare la qualità (62), ad es. attraverso *key quality indicator* riportati periodicamente agli utenti di *business*, alle funzioni di controllo e all'organo con funzione di gestione;

— la identificazione, la misurazione o la valutazione, il monitoraggio, la prevenzione o l'attenuazione dei rischi connessi con la qualità dei dati fa parte del processo di gestione dei rischi (*cfr.* Capitolo 7); in caso di acquisizione o incorporazione di soggetti esterni, la *due diligence* comprende la valutazione dell'impatto dell'operazione sulle procedure di gestione e aggregazione dei dati; l'utilizzo di procedure settoriali (contabilità, segnalazioni, antiriciclaggio, ecc.) non compromette la qualità e la coerenza complessiva dei dati aziendali; a livello consolidato, il sistema di gruppo assicura l'integrazione tra le informazioni provenienti da tutte le componenti del gruppo;

— nel caso di ricorso a un *data warehouse* aziendale a fini di analisi e *reporting*, le procedure di estrazione dei dati, di trasformazione, controllo e caricamento negli archivi accentrati — così come le funzioni di sfruttamento dei dati — sono dettagliatamente documentate, al fine di consentire la verifica sulla qualità dei dati;

— le procedure di gestione e aggregazione dei dati sono documentate, con specifica previsione delle circostanze in cui è ammessa l'immissione o la rettifica manuale di dati aziendali, registrando data, ora, autore e motivo dell'intervento, ambiente operativo interessato e i dati precedenti la modifica;

— i processi di acquisizione di dati da *information provider* esterni sono documentati e presidiati;

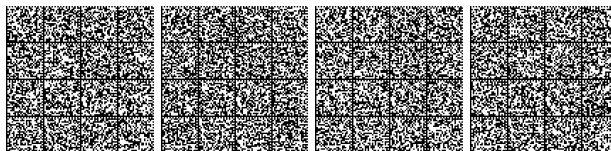
— i dati sono conservati con una granularità adeguata a consentire le diverse analisi e aggregazioni richieste dalle procedure di sfruttamento;

— i rapporti prodotti espongono le principali assunzioni e gli eventuali criteri di stima adottati (ad es., nell'ambito del monitoraggio dei rischi aziendali);

— il sistema di *reporting* consente di produrre informazioni tempestive e di qualità elevata per l'autorità di vigilanza e per il mercato.

(60) I controlli sulle registrazioni contabili verificano, tra l'altro, le procedure per l'individuazione e sistemazione delle divergenze tra saldi dei sottosistemi sezionali e quelli della contabilità generale, i processi di quadratura tra i documenti di front-office e le registrazioni giornaliere; la conferma periodica dei rapporti con controparti e clienti. Le verifiche riguardano anche l'allineamento tra i dati utilizzati per la gestione dei rischi e per la rendicontazione finanziaria.

(61) Le banche classificate, a fini SREP, nelle macro-categorie 1 e 2 (cfr. Circolare 269 del 7 maggio 2008, «Guida per l'attività di vigilanza», Sezione I, Capito I.5) individuano per i dati rilevanti (informazione al mercato, segnalazioni all'Organo di Vigilanza, valutazione dei rischi, ecc.) una o più figure aziendali responsabili di assicurare lo svolgimento dei controlli previsti e della validazione della qualità dei dati (c.d. «data owner»). Le procedure di aggregazione dei dati a fini di valutazione dei rischi aziendali sono sottoposte a validazione indipendente (ad es., da parte dell'internal audit).

(62) La qualità dei dati è valutata, in termini di completezza (registrazione di tutti gli eventi, operazioni e informazioni con i pertinenti attributi necessari per le elaborazioni), di accuratezza (assenza di distorsione nei processi di registrazione, raccolta e di successivo trattamento dei dati) e di tempestività.

Sezione VI
L'ESTERNALIZZAZIONE DEL SISTEMA INFORMATIVO

1. Tipologie di esternalizzazione.

L'esternalizzazione delle risorse e servizi ICT può assumere diverse forme a seconda del modello architetturale adottato: dall'*outsourcing* verticale (relativo a determinati processi operativi) all'*outsourcing* orizzontale di servizi trasversali come la gestione degli apparati hardware (*facility management*), lo sviluppo e la gestione del parco applicativo (*application management*), i collegamenti di rete, l'*help desk* tecnico e gli interventi di riparazione e manutenzione delle risorse ICT, fino al *full outsourcing* del complessivo sistema informativo aziendale.

Le norme nella presente Sezione si applicano ai casi di *full outsourcing* o di esternalizzazione di componenti critiche del sistema informativo, a complemento di quanto disposto in materia di *outsourcing* di funzioni aziendali nel Capitolo 7, Sezioni IV e V.

L'intermediario valuta la possibilità di ricorrere all'esternalizzazione considerando attentamente tutti i rischi (tra cui: operativi, di *compliance*, strategici e reputazionali) inerenti tale opzione, e tenendo conto della necessità, nel caso, di mettere in atto le idonee misure di contenimento.

Con particolare riferimento all'esternalizzazione di parte o tutto il sistema presso fornitori al di fuori del gruppo di appartenenza, la scelta è basata su un'analisi del rischio, che considera in primo luogo la stima dei rischi delle risorse e servizi da esternalizzare (ad es., tiene conto della classificazione dei dati e della criticità dell'operatività interessata, valutando in particolare i rischi derivanti dalla perdita del controllo diretto su componenti del sistema informativo e personale critici, nonché dei volumi delle operazioni) e quindi valuta i rischi dei possibili fornitori (ad es., condizioni finanziarie, posizionamento sul mercato, qualità e *turnover* del management e del personale, capacità di gestire la continuità operativa e di fornire accurati e tempestivi *report* direzionali sull'attività svolta, competenza ed esperienza, qualità e sicurezza nonché economicità e maturità, in un adeguato orizzonte temporale, della fornitura), la qualità dei sub-fornitori, la ridondanza delle linee di comunicazione utilizzate nonché l'affidabilità, la sicurezza e la scalabilità delle tecnologie adottate.

Nell'elaborazione del modello architetturale e delle strategie di esternalizzazione vanno considerati approcci tesi a contenere, per quanto possibile, il grado di dipendenza da specifici fornitori e partner tecnologici esterni al gruppo bancario (c.d. *vendor lock-in*), salvaguardando la possibilità di sostituire la fornitura con un'altra funzionalmente equivalente (ad es., privilegiando il ricorso a standard aperti per le connessioni, la memorizzazione e lo scambio di dati, la cooperazione applicativa) e prevedendo opportune *exit strategies* (63). Tali valutazioni tengono conto del principio di proporzionalità e dell'opportunità, per le banche di maggiore dimensione, di mantenere all'interno della banca o del gruppo competenze professionali per gestire una transizione tra modelli di *sourcing* in caso di grave necessità.

Il mantenimento nel tempo da parte del fornitore delle condizioni necessarie a fornire un servizio rispondente alle esigenze e conforme alle norme è assicurato attraverso idonei strumenti contrattuali e procedure di controllo.

2. Accordi con i fornitori e altri requisiti.

Nel caso di esternalizzazione del sistema informativo e di risorse ICT critiche, la comunicazione preventiva alla Banca d'Italia (*cfr.* Capitolo 7, Sezioni IV e V) include i risultati dell'analisi dei rischi e — limitatamente agli intermediari delle macro-categorie 1 e 2 a fini SREP — la descrizione delle *exit strategies* previste.

Il referente per l'attività esternalizzata possiede le competenze idonee per esercitare il proprio ruolo di controllo sulle componenti gestite dal fornitore di servizi.

Nei contratti con i fornitori di sistemi e servizi ICT, in aggiunta alle richiamate disposizioni del Capitolo 7, sono disciplinati al minimo i seguenti aspetti:

— l'obbligo per il fornitore di servizi di osservare la *policy* di sicurezza informatica aziendale, per quanto applicabile; il fornitore provvede al trattamento dei dati in accordo con il loro livello di classificazione, con particolare riferimento alla riservatezza;

— la proprietà di dati, software, documentazione tecnica e altre risorse ICT, con l'esclusiva per l'intermediario sui dati inerenti la clientela e i servizi ad essa forniti;

— la periodica produzione delle copie di *backup* del sistema informativo (database, transazioni, log applicativi e di sistema); l'intermediario può accedere alle copie di *backup* su richiesta;

— la ripartizione dei compiti e delle responsabilità attinenti i presidi di sicurezza per la tutela di dati, applicazioni e sistemi; i presidi sono riferiti alle principali minacce interne ed esterne, anche attraverso internet;

— le procedure di comunicazione e coordinamento in caso di incidenti di sicurezza informatica e di continuità operativa;

— la definizione di livelli di servizio coerenti con le esigenze delle applicazioni e dei processi aziendali che si avvalgono dei servizi esternalizzati;

— la predisposizione di misure di tracciamento idonee a garantire l'*accountability* e la ricostruibilità delle operazioni effettuate, almeno con riferimento alle operazioni critiche e agli accessi a dati riservati;

— il raccordo con i ruoli e le procedure definite all'interno dell'intermediario per il processo di analisi dei rischi (*cfr.* Sezione III) e per il sistema di gestione dei dati (*cfr.* Sezione V);

— la possibilità per l'intermediario di conoscere l'ubicazione dei *data center* e una indicazione del numero di addetti con accesso ai dati riservati o alle componenti critiche; tali informazioni sono periodicamente aggiornate dal fornitore di servizi;

— l'obbligo per il fornitore di servizi, una volta concluso il rapporto contrattuale e trascorso un periodo di tempo concordato, di eliminare — facendo uso di opportuni strumenti e capacità tecniche, debitamente documentati — qualsiasi copia o stralcio di dati riservati di proprietà dell'intermediario e presente su propri sistemi o supporti, in modo da escludere qualunque accesso successivo da parte del proprio personale o di terzi.

3. Indicazioni particolari.

L'intermediario pone particolare cautela nella valutazione di offerte di servizi in *outsourcing* erogati secondo modelli innovativi che prevedono la fruizione delle risorse informatiche nella forma di servizi accessibili via rete e configurabili in modo flessibile dall'utente (*cloud computing*).

Il *cloud computing* può essere implementato secondo diverse tipologie:

— *cloud privato*: ambienti interni alla società o al gruppo che permettono la condivisione di risorse ICT tra più aree e realtà aziendali; questo caso non rientra nella definizione di servizio esternalizzato;

— *community*: i servizi sono utilizzati da un ristretto numero di organizzazioni, tipicamente operanti nello stesso settore economico, che condividono analoghe necessità e obiettivi. La condivisione delle risorse informatiche è ristretta a dette organizzazioni;

— *cloud pubblico*: i servizi sono erogati a un vasto numero di utenti con funzionalità offerte in maniera aperta e condivisa. I fornitori in genere sfruttano la possibilità di condividere in modo flessibile le proprie risorse tra i diversi utenti e applicano di norma tariffe proporzionali all'utilizzo (*pay-per-use*).

Nel caso dell'acquisizione di servizi in *community* o *in cloud* pubblici i maggiori rischi potenziali possono richiedere una più elevata complessità dei controlli da predisporre, in particolare in caso di esternalizzazione di componenti critiche.

A causa della possibilità tecnica per il fornitore di spostare rapidamente e in modo trasparente all'utente le risorse dedicate ai vari clienti, è importante che le locazioni dei *data center* utilizzabili siano preventivamente comunicate. È necessario prevedere adeguati meccanismi di isolamento dei dati di un intermediario rispetto agli altri clienti, a garanzia della loro riservatezza e integrità. Il fornitore garantisce contrattualmente il rispetto dei livelli di servizio stabiliti, anche in casi di emergenza o di contesa delle risorse da parte di altri suoi clienti, e assicura la piena ricostruzione degli accessi e delle modifiche effettuate sui dati, anche per finalità ispettive. Sono concordate con il fornitore di servizi modalità di *audit* adeguate alla criticità delle risorse esternalizzate e in considerazione dell'architettura del fornitore.

(63) Anche l'acquisizione di licenze software per prodotti installati sul proprio sistema, a supporto di importanti processi aziendali trasversali, può introdurre forme di dipendenza dal fornitore, a seguito di vincoli tecnologici o contrattuali che impongano il ricorso al fornitore o a società collegate per la manutenzione o rendano assai ardua la sostituzione del prodotto. Tali considerazioni rientrano tra gli elementi essenziali nel processo di selezione delle soluzioni software.

ALLEGATO A

DOCUMENTI AZIENDALI PER LA GESTIONE
E IL CONTROLLO DEL SISTEMA INFORMATIVO

Documento	Approvazione	Aggiornamento	Note
DOCUMENTI DI *POLICY* E STANDARD AZIENDALI			
Documento di indirizzo strategico	Organo con funzione di supervisione strategica	In dipendenza della periodicità dei piani strategici aziendali (3 – 5 anni)	Contiene (cfr. Sezione II, par. 1): – modello di riferimento architetturale – strategie di *sourcing* – propensione al rischio informatico
Metodologia di analisi del rischio informatico	Organo con funzione di supervisione strategica	In base alla necessità	
Policy di sicurezza informatica	Organo con funzione di supervisione strategica	In base alla necessità	
Organigramma della funzione ICT	Organo con funzione di supervisione strategica	In base alla necessità	Include il disegno dei processi di gestione dell'ICT (cfr. Sezione II, par. 2)
Standard di *data governance*	Organo con funzione di gestione	Periodicità definita	
ALTRI DOCUMENTI ESSENZIALI PER LA GESTIONE E LO SVILUPPO DEI SISTEMI ICT			
Procedura di gestione dei cambiamenti	Organo con funzione di gestione	In base alla necessità	
Procedura di gestione degli incidenti	Organo con funzione di gestione	In base alla necessità	
Piano operativo	Organo con funzione di gestione	Annuale	
VALUTAZIONI AZIENDALI			
Rapporto sintetico su adeguatezza e costi dell'ICT	Organo con funzione di supervisione strategica	Annuale	
Rapporto sintetico sulla situazione del rischio informatico	Organo con funzione di supervisione strategica	Annuale	
Rapporti dell'*internal audit* e delle altre funzioni responsabili della valutazione della sicurezza	Organo con funzione di supervisione strategica	Almeno annuale	

TITOLO V

CAPITOLO 9
LA CONTINUITÀ OPERATIVA

1. Destinatari.

L'Allegato A, Sezione II (Requisiti per tutti gli operatori) si applica alle banche e ai gruppi bancari.

L'Allegato A, Sezione III (Requisiti particolari per i processi a rilevanza sistemica) si applica, in aggiunta ai requisiti previsti nella Sezione II dell'Allegato A, ai soggetti, individuati nominativamente, con apposita comunicazione, fra i gruppi bancari e le banche non appartenenti a gruppi con una quota di mercato, calcolata sul totale attivo, superiore al 5 per cento del totale del sistema bancario.

Nell'ambito dei gruppi bancari, i requisiti particolari si applicano alla capogruppo, alle singole controllate bancarie italiane con totale attivo superiore a 5 miliardi di euro e alle altre controllate bancarie, finanziarie e strumentali che, indipendentemente dalla dimensione e localizzazione, svolgono in misura rilevante i processi a rilevanza sistemica o danno un supporto essenziale a questi ultimi.

Possono essere altresì assoggettati ai requisiti particolari gli operatori, incluse le succursali italiane di banche estere, che, su base individuale, detengono una quota di mercato superiore al 5 per cento in almeno uno dei seguenti segmenti del sistema finanziario italiano: regolamento lordo in moneta di banca centrale, liquidazione di strumenti finanziari, servizi di controparte centrale, sistemi multilaterali di scambio di depositi interbancari in euro, aste BCE, operazioni di finanziamento del Tesoro effettuate tramite asta, mercato dei pronti contro termine all'ingrosso su titoli di Stato, pagamento delle pensioni sociali, bollettini postali.

2. Fonti normative.

La materia è regolata:

— dalla direttiva del Parlamento europeo e del Consiglio 2013/36/UE del 26 giugno 2013, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE;

— dai seguenti articoli del TUB:

• art. 51, il quale prevede che le banche inviino alla Banca d'Italia, con le modalità e i tempi da essa stabiliti, le segnalazioni periodiche nonché ogni dato e documento richiesti;

• art. 53, comma 1, lett. *d)*, che attribuisce alla Banca d'Italia, in conformità delle delibere del CICR, il potere di emanare disposizioni di carattere generale in materia di organizzazione amministrativa e contabile e controlli interni delle banche;

• art. 67, comma 1, lett. *d)*, che attribuisce alla Banca d'Italia, in conformità delle delibere del CICR, il potere di impartire alla capogruppo di un gruppo bancario disposizioni concernenti il gruppo complessivamente considerato o i suoi componenti aventi ad oggetto l'organizzazione amministrativa e contabile e i controlli interni;

— dalla delibera del CICR del 2 agosto 1996, come modificata dalla delibera del 23 marzo 2004, in materia di organizzazione amministrativa e contabile e controlli interni delle banche e dei gruppi bancari.

Si tiene anche conto delle *Guidelines on Internal Governance*, dell'EBA/CEBS del 27 settembre 2011.

3. Banche soggette ai requisiti applicabili a tutti gli operatori (Allegato A, Sezione II).

Fermo restando quanto previsto nell'Allegato A, Sezione II, si precisa quanto segue:

— i gruppi bancari — coerentemente con quanto previsto nel Capitolo 7, Sezione V (Il RAF, il sistema dei controlli interni e l'esternalizzazione nei gruppi bancari) — possono definire e gestire i piani di continuità operativa in modo accentrato per l'intero gruppo o decentrato per singola società. In ogni caso la capogruppo assicura che tutte le controllate siano dotate di piani di continuità operativa e verifica la coerenza degli stessi con gli obiettivi strategici del gruppo in tema di contenimento dei rischi. A livello di gruppo sono stabiliti controlli sul raggiungimento degli obiettivi di continuità operativa definiti per l'intero gruppo e le singole componenti;

— i compiti e le responsabilità degli organi aziendali indicati ai punti *a)*, *b)*, *c)*, *d)*, ed *e)* dell'Allegato A, Sezione II, par. 3.1, rientrano nelle competenze dell'organo con funzione di supervisione strategica; i compiti e le responsabilità indicati nei punti *f)* e *g)* del menzionato paragrafo, spettano all'organo con funzione di gestione;

— le banche segnalano alla Banca d'Italia, tra le «cariche rilevanti a fini di Vigilanza» previste nella procedura «organi sociali» (Or. So.), il nome del responsabile del piano di continuità operativa (*cfr.* Allegato A, Sezione II, par. 0);

— la procedura per la dichiarazione dello stato di crisi (*cfr.* Allegato A, Sezione II, par. 3.1) è definita in raccordo con il processo di gestione degli incidenti di sicurezza informatica (*cfr.* Capitolo 8, Sezione IV, par. 6) e delle altre tipologie di incidenti;

— le verifiche annuali dei sistemi informativi (*cfr.* Allegato A, Sezione II, par. 3.5) prevedono anche l'operatività *on-line* di almeno una succursale;

— le previsioni in materia di Esternalizzazione, infrastrutture e controparti rilevanti (*cfr.* Allegato A, Sezione II, par. 3.7), si applicano coerentemente con quanto previsto dalle disposizioni in materia di esternalizzazione previste nei Capitoli 7 e 8;

— in caso di situazione di crisi che non assumano rilevanza sistemica per il sistema finanziario, le banche e i gruppi bancari contattano, al fine di agevolare il coordinamento degli interventi, la Banca d'Italia.

4. Banche soggette ai requisiti particolari per i processi a rilevanza sistemica (Allegato A, Sezione III).

Fermo restando quanto previsto nell'Allegato A, Sezione III, si precisa quanto segue:

— per i gruppi bancari, la capogruppo promuove e coordina l'attuazione degli interventi di adeguamento dei piani di continuità operativa relativi ai processi a rilevanza sistemica e garantisce nel continuo il rispetto da parte di tutte le controllate interessate dei requisiti previsti per i processi a rilevanza sistemica. Nomina un responsabile unico di tali attività, con competenze estese all'intero gruppo (*cfr.* Allegato A, Sezione III, par. 2.2);

— per le succursali italiane di intermediari esteri, il coordinamento del piano di continuità operativa relativo ai processi a rilevanza sistemica è assicurato dalle succursali stesse, in stretto raccordo con le strutture che gestiscono la continuità operativa a livello centrale o di area geografica.

ALLEGATO A

REQUISITI PER LA CONTINUITÀ OPERATIVA

Sezione I
DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa.

La crescente complessità dell'attività finanziaria, l'intenso utilizzo della tecnologia dell'informazione e i nuovi scenari di rischio richiedono che gli operatori rafforzino l'impegno a garantire adeguati livelli di continuità operativa.

A tal fine, essi adottano un approccio esteso che, partendo dalla identificazione dei processi aziendali critici, definisca per ciascuno di essi presidi organizzativi e misure di continuità operativa commisurati ai livelli di rischio.

Le concrete misure da adottare tengono conto degli standard e *best practices* definiti a livello internazionale e/o definiti nell'ambito degli organismi di categoria.

2. Definizioni.

— «*CODISE (continuità di servizio)*»: struttura per il coordinamento delle crisi operative della piazza finanziaria italiana presieduta dalla Banca d'Italia;

— «*crisi*»: situazione formalmente dichiarata di interruzione o deterioramento di uno o più processi critici o a rilevanza sistemica in seguito a incidenti o catastrofi;

— «*escalation*»: conduzione della gestione di un incidente caratterizzata da un aumento progressivo dei livelli aziendali coinvolti, fino a giungere, ove necessario, all'organo di amministrazione;

— «*emergenza*»: situazione originata da incidenti o catastrofi che colpiscono l'operatore, caratterizzata dalla necessità di adottare misure tecniche e gestionali eccezionali, finalizzate al tempestivo ripristino della normale operatività;

— «*gestione della continuità operativa*»: insieme delle iniziative volte a ridurre a un livello ritenuto accettabile i danni conseguenti a incidenti o catastrofi che colpiscono direttamente o indirettamente un operatore;

— «*piano di continuità operativa*»: documento che formalizza i principi, fissa gli obiettivi, descrive le procedure e individua le risorse, per la gestione della continuità operativa dei processi aziendali critici e a rilevanza sistemica. Esso è generalmente articolato in piani settoriali;

— «*piano di disaster recovery*»: documento che stabilisce le misure tecniche e organizzative per fronteggiare eventi che provochino la indisponibilità dei centri di elaborazione dati. Il piano di *disaster recovery*, finalizzato a consentire il funzionamento delle procedure informatiche rilevanti in siti alternativi a quelli di produzione, costituisce parte integrante del piano di continuità operativa;

— «*punto di ripristino*»: istante di salvataggio dei dati fino al quale è garantita l'integrità degli stessi nei siti primari e alternativi;

— «*sito alternativo*»: infrastruttura che consente all'operatore di continuare a svolgere i propri processi critici e a rilevanza sistemica, anche in caso di incidenti o disastri che rendano indisponibile il sito primario;

— «*sito primario*»: infrastruttura presso la quale sono normalmente svolte le attività dell'operatore;

— «*tempo di ripristino di un processo*»: periodo che intercorre fra il momento in cui l'operatore dichiara lo stato crisi e l'istante in cui il processo è ripristinato a un livello di servizio predefinito. Esso è costituito dai tempi di:

• analisi degli eventi e decisione delle azioni da intraprendere, prima di effettuare gli interventi;

• ripartenza del processo, attraverso l'attuazione degli interventi tecnici e organizzativi e la successiva verifica sulla possibilità di rendere nuovamente disponibili i servizi senza danni e in condizioni di sicurezza.

Sezione II
REQUISITI PER TUTTI GLI OPERATORI

1. Ambito del piano di continuità operativa.

Gli operatori definiscono un piano di continuità operativa per la gestione di situazioni di crisi conseguenti a incidenti di portata settoriale, aziendale ovvero a catastrofi estese che colpiscono l'operatore o le sue controparti rilevanti (altre società del gruppo; principali fornitori; clientela primaria; specifici mercati finanziari; sistemi di regolamento, compensazione e garanzia).

I piani di continuità operativa prevedono soluzioni, non solo basate su misure tecnico-organizzative finalizzate alla salvaguardia degli archivi elettronici e al funzionamento dei sistemi informativi, ma che considerino anche ipotesi di crisi estesa e blocchi prolungati delle infrastrutture essenziali in modo da assicurare la continuità operativa dell'operatore in caso di eventi disastrosi.

Laddove alcuni processi critici siano svolti da soggetti specializzati appartenenti al gruppo (ad es., allocazione della funzione informatica o del *back-office* presso una società strumentale), i relativi presidi di continuità operativa costituiscono parte integrante dei piani di continuità operativa degli operatori.

Il piano di continuità operativa si inquadra nella complessiva politica di governo dei rischi dell'operatore; esso tiene conto delle vulnerabilità esistenti e delle misure preventive poste in essere per garantire il raggiungimento degli obiettivi aziendali.

Il piano di continuità operativa prende in considerazione diversi scenari di crisi basati almeno sui seguenti fattori di rischio, conseguenti a eventi naturali o attività umana, inclusi danneggiamenti gravi da parte di dipendenti:

— distruzione o inaccessibilità di strutture nelle quali sono allocate unità operative o apparecchiature critiche;

— indisponibilità di sistemi informativi critici;

— indisponibilità di personale essenziale per il funzionamento dei processi aziendali;

— interruzione del funzionamento delle infrastrutture (tra cui energia elettrica, reti di telecomunicazione, reti interbancarie, mercati finanziari);

— alterazione o perdita di dati e documenti critici.

Il piano di continuità operativa indica le procedure per il rientro dall'emergenza, con particolare attenzione alla rilevazione dei danni, alla gestione di tutte le operazioni di rientro, alla verifica dell'operatività per i servizi ripristinati.

2. Analisi di impatto.

L'analisi di impatto, preliminare alla stesura del piano di continuità operativa e periodicamente aggiornata, individua il livello di rischio relativo ai singoli processi aziendali e pone in evidenza le conseguenze della interruzione del servizio. I rischi residui, non gestiti dal piano di continuità operativa, sono documentati ed esplicitamente accettati dagli organi aziendali competenti. L'allocazione delle risorse e le priorità di intervento sono correlate al livello di rischio.

L'analisi di impatto tiene conto dei parametri caratteristici della struttura organizzativa e dell'operatività aziendale, tra cui:

— le specificità — in termini di probabilità di catastrofe — connesse con la localizzazione dei siti rilevanti (ad es., sismicità dell'area, dissesto idrogeologico del territorio, vicinanza ad insediamenti industriali pericolosi, prossimità ad aeroporti o a istituzioni con alto valore simbolico);

— i profili di concentrazione geografica (ad es., presenza di una pluralità di operatori nei centri storici di grandi città);

— la complessità dell'attività tipica o prevalente e il grado di automazione raggiunto;

— le dimensioni aziendali e l'articolazione territoriale dell'attività;

— il livello di esternalizzazione di funzioni rilevanti (ad es., *outsourcing* del sistema informativo o del *back-office*);

— l'assetto organizzativo in termini di accentramento o decentramento di processi critici;

— i vincoli derivanti da interdipendenze, anche tra e con fornitori, clienti, altri operatori.

L'analisi di impatto prende in considerazione, oltre ai rischi operativi, anche gli altri rischi (ad es., di mercato e di liquidità).

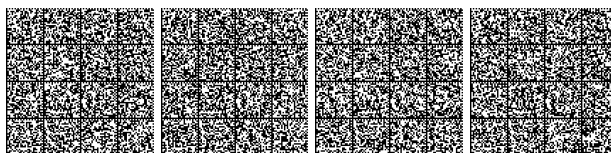
3. Definizione del piano di continuità operativa e gestione delle crisi.

3.1. *Ruolo degli organi aziendali*.

Il tema della continuità operativa è adeguatamente valutato a tutti i livelli di responsabilità. In tale ambito, l'organo di amministrazione:

a) stabilisce gli obiettivi e le strategie di continuità operativa del servizio;

b) assicura risorse umane, tecnologiche e finanziarie adeguate per il conseguimento degli obiettivi fissati;

c) approva il piano di continuità operativa e le successive modifiche a seguito di adeguamenti tecnologici ed organizzativi, accettando i rischi residui non gestiti dal piano di continuità operativa;

d) è informato, con frequenza almeno annuale, sugli esiti dei controlli sull'adeguatezza del piano nonché delle verifiche delle misure di continuità operativa;

e) nomina il responsabile del piano di continuità operativa;

f) promuove lo sviluppo, il controllo periodico del piano di continuità operativa e l'aggiornamento dello stesso a fronte di rilevanti innovazioni organizzative, tecnologiche e infrastrutturali nonché nel caso di lacune o carenze riscontrate ovvero di nuovi rischi sopravvenuti;

g) approva il piano annuale delle verifiche delle misure di continuità operativa ed esamina i risultati delle prove documentati in forma scritta.

L'organo con funzione di controllo ha la responsabilità di vigilare sulla completezza, adeguatezza, funzionalità e affidabilità del piano di continuità operativa.

L'attività svolta e le decisioni assunte sono adeguatamente documentate.

3.2. *I processi critici*.

Gli operatori identificano in modo circostanziato i processi relativi a funzioni aziendali di particolare rilevanza che, per l'impatto dei danni conseguenti alla loro indisponibilità, necessitano di elevati livelli di continuità operativa da conseguire mediante misure di prevenzione e con soluzioni di continuità operativa da attivare in caso di incidente.

A tal fine, sono considerati con particolare attenzione i processi che attengono alla gestione dei rapporti con la clientela, ivi incluse imprese e pubbliche amministrazioni, e alla registrazione dei fatti contabili.

Per ciascun processo critico sono individuati il responsabile, le procedure informatiche di supporto, il personale addetto, le strutture logistiche interessate, le infrastrutture tecnologiche e di comunicazione utilizzate.

Il responsabile del processo individua, in accordo con gli indirizzi strategici e con le regole stabilite nel piano di continuità operativa, il tempo di ripristino del processo e collabora attivamente alla realizzazione delle misure di continuità operativa.

3.3. *La responsabilità del piano di continuità operativa*.

Il responsabile del piano di continuità operativa aziendale ha una posizione gerarchico-funzionale adeguata. Il responsabile cura lo sviluppo del piano di continuità operativa, ne assicura l'aggiornamento nel continuo, a fronte di cambiamenti organizzativi o tecnologici rilevanti, e ne verifica l'adeguatezza, con cadenza almeno annuale. Tale figura tiene inoltre i contatti con la Banca d'Italia in caso di crisi.

Laddove il piano di continuità operativa sia articolato in piani settoriali, gli operatori individuano i referenti per ciascuno di essi. I referenti dei piani settoriali (64) coordinano, per gli aspetti di competenza, i lavori per la definizione e la manutenzione dei piani, per l'attuazione delle misure previste nello stesso e per la conduzione delle verifiche. Prima dell'attivazione di nuovi sistemi o processi operativi, essi definiscono le opportune modifiche dei piani.

3.4. *Il contenuto del piano di continuità operativa.*

Il piano di continuità operativa documenta i presupposti e le modalità per la dichiarazione dello stato di crisi, l'organizzazione e le procedure da seguire in situazione di crisi, l'*iter* per la ripresa della normale operatività.

Il piano di continuità operativa attribuisce l'autorità di dichiarare lo stato di crisi e stabilisce la catena di comando incaricata di gestire l'azienda in circostanze eccezionali. Sono previste misure di *escalation* rapide che consentano, una volta assunta consapevolezza della portata dell'incidente, di dichiarare lo stato di crisi in tempi brevi.

I processi per la gestione degli incidenti e per la dichiarazione e gestione dello stato di crisi sono formalizzati e strettamente integrati fra loro. Anche a tal fine, sono esplicitamente individuati i membri della struttura preposta alla gestione della crisi (ad es., comitato di crisi), il responsabile della stessa struttura, la catena di comando, le modalità interne di comunicazione e le responsabilità attribuite alle funzioni aziendali interessate.

Il piano di continuità operativa stabilisce i tempi di ripristino dei processi critici.

Il piano di continuità operativa individua i siti alternativi, prevede spazi e infrastrutture logistiche e di comunicazione adeguate per il personale coinvolto nella crisi, stabilisce le regole di conservazione delle copie dei documenti importanti (ad es., i contratti) in luoghi remoti rispetto ai documenti originali.

Con riferimento ai sistemi informativi centrali e periferici, il piano di continuità operativa integra il piano di *disaster recovery* (65). In quest'ultimo sono fornite indicazioni su modalità e frequenza di generazione delle copie degli archivi di produzione, nonché sulle procedure per il ripristino presso i siti alternativi.

La frequenza dei *back-up* è correlata alle dimensioni e alle funzioni (66) dell'operatore; gli archivi di produzione dei processi critici sono duplicati almeno giornalmente. Sono assunte cautele per il tempestivo trasporto e la conservazione delle copie elettroniche in siti a elevata sicurezza fisica posti in luoghi remoti rispetto ai sistemi di produzione (67).

Il piano di continuità operativa definisce le modalità di comunicazione con la clientela, le controparti rilevanti, le autorità e i media.

I siti alternativi possono dover essere utilizzati, in caso di necessità, anche per periodi prolungati.

3.5. *Le verifiche.*

Le modalità di verifica delle misure di continuità operativa dipendono dalla criticità dei processi e dai rischi ravvisati; di conseguenza sono ipotizzabili differenti frequenze e livelli di dettaglio delle prove. In alcuni casi può essere sufficiente la simulazione parziale dell'evento catastrofico; per i processi critici le verifiche prevedono il coinvolgimento degli utenti finali, dei fornitori di servizi e, qualora possibile, delle controparti rilevanti.

Con frequenza almeno annuale sono svolte verifiche complessive, basate su scenari il più possibile realistici, del ripristino della operatività dei processi critici in condizioni di crisi, riscontrando la capacità dell'organizzazione di attuare nei tempi previsti le misure definite nel piano di continuità operativa.

In particolare, le verifiche annuali dei sistemi informativi prevedono l'attivazione dei collegamenti di rete presso il sito alternativo e l'esecuzione delle procedure *batch* con controllo della funzionalità e delle prestazioni dei siti alternativi. Le prove sono preferibilmente realizzate con dati di produzione.

I risultati delle verifiche sono documentati per iscritto, portati all'attenzione degli organi aziendali competenti e inviati, per le parti di competenza, alle unità operative coinvolte e alla funzione di *audit*. A fronte di carenze riscontrate nelle prove sono tempestivamente avviate le opportune azioni correttive.

3.6. *Le risorse umane.*

Il piano di continuità operativa individua il personale essenziale per assicurare la continuità operativa dei processi critici e fornisce allo stesso indicazioni dettagliate sulle attività da porre in essere in caso di crisi.

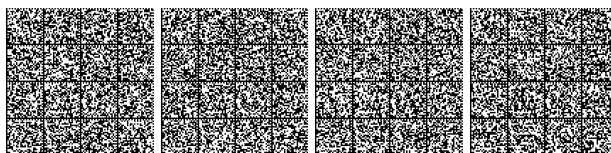
Le procedure di continuità operativa sono chiare e dettagliate, in modo da poter essere eseguite anche da risorse non impegnate nell'ordinaria attività nei processi cui si riferiscono.

---

(64) Ove il piano di continuità operativa non sia articolato in piani settoriali, tali attività sono svolte dal responsabile del piano di continuità operativa.

(65) In caso di outsourcing di componenti critiche del sistema informativo si applica quanto indicato al par. 3.7.

(66) Ad esempio, nel caso in cui svolga il ruolo di tramite per partecipanti indiretti.

(67) Per i processi non critici sono comunque realizzati meccanismi per acquisire e gestire regolarmente copie di riserva dei dati e del software, al fine di assicurare l'integrità e la disponibilità delle informazioni. Per i siti alternativi off-line, in cui non siano presenti archivi di dati ovvero questi non siano allineati in tempo reale ai dati di produzione, sono definite modalità e tempi per l'allineamento con i sistemi di produzione dopo il loro ripristino.

Il personale coinvolto nel piano di continuità operativa è addestrato sulle misure di continuità operativa, accede alla lista di contatto e alla documentazione necessaria per operare in situazione di crisi, ha dimestichezza con i siti alternativi e con le apparecchiature in essi contenute, partecipa alle sessioni di verifica delle misure di continuità operativa.

Va valutata l'opportunità di frazionare l'attività connessa con i processi critici in più siti ovvero di organizzare il lavoro del personale su turni.

3.7. *Esternalizzazione, infrastrutture e controparti rilevanti.*

In caso di esternalizzazione di funzioni aziendali connesse allo svolgimento di processi critici, il piano di continuità operativa prevede le misure da attuare in caso di crisi con impatto rilevante sull'operatore o sul fornitore di servizi.

Nel contratto sono formalizzati i livelli di servizio assicurati in caso di crisi e le soluzioni di continuità operativa poste in atto dal fornitore di servizi, adeguati al conseguimento degli obiettivi aziendali e coerenti con le prescrizioni della Banca d'Italia. Sono altresì stabilite le modalità di partecipazione, diretta o per il tramite di comitati utente, alle verifiche dei piani di continuità operativa dei fornitori.

L'operatore acquisisce i piani di continuità operativa del fornitore di servizi o dispone di informazioni adeguate, al fine di valutare la qualità delle misure previste e di integrarle con le soluzioni di continuità operativa realizzate all'interno. Il fornitore di servizi comunica tempestivamente all'operatore il verificarsi di incidenti al fine di consentire la pronta attivazione delle relative procedure di continuità operativa.

Il piano di continuità operativa dell'operatore considera l'eventualità che le principali infrastrutture tecnologiche e finanziarie e le controparti rilevanti siano colpite da un evento catastrofico e stabilisce le misure per gestire i problemi conseguenti; la capacità di comunicare con i siti alternativi di tali soggetti è verificata periodicamente.

Per i servizi essenziali dell'operatore, va valutata la possibilità di prevedere il ricorso, in casi di emergenza, a fornitori alternativi.

Nel caso in cui il fornitore abbia impegnato le stesse risorse per fornire analoghi servizi ad altre aziende, in particolare se situate nella stessa zona, sono stabilite cautele contrattuali per evitare il rischio che, in caso di esigenze concomitanti di altre organizzazioni, le prestazioni degenerino o il servizio si renda di fatto indisponibile.

3.8. *Controlli.*

Il piano di continuità operativa e il relativo processo di aggiornamento sono oggetto di regolare verifica da parte della funzione di revisione interna. L'*internal audit* prende visione dei programmi di verifica, assiste alle prove e ne controlla i risultati, proponendo modifiche al piano di continuità operativa sulla base delle mancanze riscontrate.

In tale ambito, particolare attenzione è posta all'analisi dei criteri di *escalation*. In caso di incidenti, la funzione di *audit* verifica la congruità dei tempi rilevati per la dichiarazione dello stato di crisi. La funzione di revisione interna è anche coinvolta nel controllo dei piani di continuità operativa dei fornitori di servizi esternalizzati e degli altri fornitori critici; essa può decidere di fare affidamento sulle strutture di questi ultimi se ritenute professionali, indipendenti e trasparenti quanto ai risultati dei controlli. L'*internal audit* esamina i contratti per accertare che il livello di tutela sia adeguato agli obiettivi e agli standard aziendali.

Gli operatori considerano l'opportunità di sottoporre il piano di continuità operativa alla revisione da parte di competenti terze parti indipendenti.

3.9. *Comunicazioni alla Banca d'Italia.*

In caso di crisi, successivamente al ripristino dei processi critici, l'operatore fornisce alla Banca d'Italia valutazioni circa l'impatto dell'evento sulla operatività delle strutture centrali e periferiche e sui rapporti con la clientela e le controparti.

Sezione III
REQUISITI PARTICOLARI PER I PROCESSI A RILEVANZA SISTEMICA

1. Premessa.

L'operatività del sistema finanziario nel suo complesso si basa sul corretto funzionamento dei maggiori operatori e sulla loro capacità di erogare i servizi essenziali nei comparti dei sistemi di pagamento e dell'accesso ai mercati finanziari.

A tali soggetti la Banca d'Italia può chiedere il rispetto di requisiti di continuità operativa più stringenti rispetto a quelli previsti per la generalità degli operatori, in particolare con riferimento ai tempi di ripristino per i processi a rilevanza sistemica (*cfr.* par. 2.1), alla localizzazione dei siti alternativi, alle risorse previste per gestire le situazioni di crisi.

La Banca d'Italia individua nominativamente gli operatori ai quali si applicano i requisiti particolari, richiede adeguamenti dei piani di continuità operativa, verifica le soluzioni adottate. Tali operatori partecipano alle iniziative per il coordinamento della continuità operativa del sistema finanziario del CODISE.

2. Definizione del piano di continuità operativa e gestione delle crisi.

2.1. *Processi a rilevanza sistemica.*

I processi ad alta criticità nel sistema finanziario italiano che, per un effetto di contagio, possono provocare il blocco dell'operatività dell'intera piazza finanziaria nazionale si concentrano nei sistemi di pagamento e nelle procedure per l'accesso ai mercati finanziari.

Tali processi sono denominati, ai fini delle presenti disposizioni, «processi a rilevanza sistemica» per la continuità operativa del sistema finanziario italiano. La Banca d'Italia comunica a ciascun operatore i processi a rilevanza sistemica di pertinenza. Si tratta di un complesso strutturato di attività finalizzate all'erogazione dei seguenti servizi:

— servizi connessi con i sistemi di regolamento lordo in moneta di banca centrale e con i sistemi di gestione accentrata, compensazione, garanzia e liquidazione degli strumenti finanziari. Sono inclusi: regolamento lordo in moneta di banca centrale (Target 2), liquidazione di strumenti finanziari (Express II), gestione accentrata di strumenti finanziari, sistemi di riscontro e rettifica giornalieri, servizi di controparte centrale;

— servizi connessi con l'accesso ai mercati rilevanti per regolare la liquidità del sistema finanziario. Sono inclusi: sistemi multilaterali di scambio di depositi interbancari in euro (e-Mid), aste BCE, operazioni di finanziamento del Tesoro effettuate tramite asta, Mercato dei pronti contro termine all'ingrosso su titoli di Stato (MTS comparto PCT);

— servizi di pagamento al dettaglio a larga diffusione tra il pubblico. Sono inclusi: bollettini postali, pagamento delle pensioni sociali, erogazione del contante;

— servizi strettamente funzionali al soddisfacimento di fondamentali esigenze di liquidità degli operatori economici, il cui blocco ha rilevanti effetti negativi sull'operatività degli stessi. Sono inclusi: gestione delle infrastrutture telematiche per l'erogazione del contante tramite terminale ATM, supporto ad applicazioni e servizi rientranti nell'ambito della «Convenzione per la partecipazione al Sistema per la trasmissione telematica di dati» (SITRAD).

2.2. *Responsabilità.*

L'operatore:

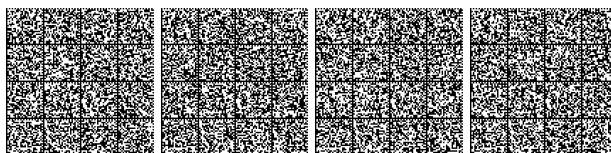
— attua gli interventi di adeguamento dei piani di continuità operativa relativi ai processi a rilevanza sistemica;

— garantisce nel continuo il rispetto dei requisiti particolari;

— nomina un responsabile unico di tali attività.

2.3. *Scenari di rischio.*

Gli scenari di rischio rilevanti per la continuità operativa dei processi a rilevanza sistemica sono documentati e costantemente aggiornati. Essi includono, in aggiunta a quanto previsto per tutti gli operatori: eventi catastrofici con distruzioni fisiche su larga scala, a dimensio-

ne metropolitana o superiore, che investano infrastrutture essenziali dell'operatore e di terzi; situazioni di crisi gravi anche non connesse ad eventi con distruzioni materiali (ad es., pandemie, attacchi biologici, attacchi informatici su larga scala).

2.4. *Siti alternativi.*

I siti alternativi per i processi a rilevanza sistemica sono situati a congrua distanza dai siti primari in modo da assicurare un elevato grado di indipendenza tra i due insediamenti.

In generale, i siti alternativi sono ubicati all'esterno dell'area metropolitana nella quale sono presenti i siti primari; inoltre, essi utilizzano servizi (telecomunicazioni, energia, acqua, ecc.) distinti da quelli impiegati in produzione. Laddove ciò non avvenga è necessaria una valutazione rigorosa, supportata da pareri di parti terze qualificate (ad es., Protezione Civile, accademici, professionisti) e compiutamente documentata, che il rischio di indisponibilità contemporanea dei siti primari e alternativi è trascurabile.

I siti alternativi dei sistemi informativi sono configurati con capacità adeguata, all'occorrenza, a gestire volumi di attività attestati sui picchi massimi riscontrati nel corso dell'operatività ordinaria.

2.5. *Tempi di ripristino e percentuali di disponibilità.*

Il tempo di ripristino per i processi a rilevanza sistemica non supera le quattro ore. Il tempo di ripartenza per i processi a rilevanza sistemica non supera le due ore.

Se un evento catastrofico che colpisce un operatore determina un blocco dei processi a rilevanza sistemica di altri operatori, questi ultimi ripristinano i propri processi sistemici entro due ore dalla ripartenza dell'operatore colpito in prima istanza.

Nel caso in cui gli scenari (*cfr*. par. 2.3) determinino impatti particolarmente gravi, gli obiettivi di ripristino indicati possono subire un adattamento che sarà segnalato agli operatori interessati dalla Banca d'Italia, tenuto conto delle indicazioni condivise nel CODISE.

Con riferimento ai sistemi informativi, sono considerate adeguate le soluzioni basate su architetture tecnologiche che effettuino la duplicazione in linea dei dati operativi in modo da eliminare o ridurre al minimo la perdita di informazioni. A tal fine l'intervallo di tempo che intercorre fra il punto di ripristino e il momento dell'incidente è pari o prossimo a zero.

È previsto, anche in caso di situazioni estreme, un ripristino quanto più possibile immediato dei processi a rilevanza sistemica, anche facendo ricorso a procedure a bassa integrazione nei processi aziendali, purché presidiate dal punto di vista della sicurezza (ad es., mediante l'utilizzo di PC *off-line*, fax, contatti telefonici con controparti selezionate), in particolare per gestire le esigenze essenziali di liquidità.

2.6. *Risorse.*

Il piano di continuità operativa individua le risorse — umane, tecnologiche e logistiche — necessarie per l'operatività dei processi a rilevanza sistemica. Occorre garantire — con misure organizzative, mediante accordi con terzi, con la duplicazione del personale o con altri provvedimenti documentati — la presenza nei siti alternativi, all'occorrenza, del personale necessario per l'operatività dei processi a rilevanza sistemica. Va evitata la concentrazione, nello stesso luogo e allo stesso tempo, del personale chiave.

2.7. *Verifiche.*

Sono effettuate, con frequenza almeno annuale, verifiche accurate sui presidi delle misure di continuità operativa dei processi a rilevanza sistemica. Viene assicurata la partecipazione attiva ai test e alle simulazioni di sistema organizzati o promossi dalle autorità, dai mercati e dalle principali infrastrutture finanziarie.

3. Comunicazioni alla Banca d'Italia.

In caso di incidenti che possano avere impatti rilevanti sui processi a rilevanza sistemica, la dichiarazione dello stato di crisi prevede l'immediata richiesta di attivazione del CODISE con una prima valutazione degli operatori potenzialmente danneggiati.

In caso di crisi, successivamente al ripristino dei processi a rilevanza sistemica, l'operatore fornisce con tempestività alla Banca d'Italia valutazioni circa l'impatto dell'evento sulla operatività delle strutture centrali e periferiche e sui rapporti con la clientela e le controparti.

Gli operatori sistemici inviano alla Banca d'Italia un'informativa annuale sulle principali caratteristiche del piano di continuità operativa, sugli adeguamenti e integrazioni intervenuti in corso d'anno, sulle verifiche da parte dell'*internal audit*, sui principali incidenti e sulle criticità ricorrenti.

13A06294

MINISTERO DELL'AMBIENTE E DELLA TUTELA DEL TERRITORIO E DEL MARE

Non assoggettabilità a V.I.A. del progetto nuove rampe di uscita dell'Autostrada A3 Napoli-Salerno previste dal programma di interventi Pompei 2000 nel Comune di Torre Annunziata, presentato dalla Società Pompei 2000 p.A., in Roma.

Con determinazione direttoriale DVA-2013-0016072 del 9 luglio 2013, della Direzione generale per le Valutazioni Ambientali del Ministero dell'Ambiente e della Tutela del Territorio e del Mare è stata disposta la non assoggettabilità a V.I.A. del progetto nuove rampe di uscita dell'Autostrada A3 Napoli-Salerno previste dal programma di interventi Pompei 2000 nel Comune di Torre Annunziata, presentato dalla Società Pompei 2000 p.A. con sede in via Vittorio Veneto 7, 00187 Roma.

Il testo integrale della citata determinazione direttoriale è disponibile sul sito del Ministero dell'Ambiente e della Tutela del Territorio e del Mare: http://www.va.minambiente.it/provvedimenti/provvedimentivasvia/elencoverificaassoggettabilitavia.aspx"; detta determinazione direttoriale può essere impugnata dinanzi al TAR entro 60 giorni, o con ricorso al Capo dello Stato entro 120 giorni, a decorrere dalla data della pubblicazione del presente estratto nella *Gazzetta Ufficiale*.

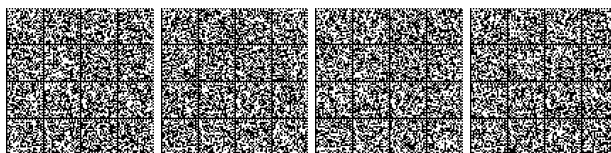
13A06321

MINISTERO DELLO SVILUPPO ECONOMICO

Programma operativo interregionale "Energie rinnovabili e risparmio energetico" (FESR) 2007 - 2013: Approvazione dell' elenco delle iniziative ammesse a finanziamento nell'ambito del Progetto JUSTICE.

Con decreto del 10 giugno 2013 è stato approvato l'elenco delle iniziative ammesse a finanziamento nell'ambito del Progetto Justice - «Join Us To Increase Clean Energy» - che promuove, nell'ambito del POI Energie Rinnovabili e Risparmio Energetico FESR 2007-2013 - linea di attività 1.3 - la produzione di energia da fonti rinnovabili nell'ambito dell'efficientamento energetico degli edifici pubblici.

Il decreto è consultabile sul sito istituzionale del Ministero all'indirizzo www.sviluppoeconomico.gov.it

13A06332

RETTIFICHE

Avvertenza.— L'**avviso di rettifica** dà notizia dell'avvenuta correzione di errori materiali contenuti nell'originale o nella copia del provvedimento inviato per la pubblicazione alla *Gazzetta Ufficiale*. L'**errata corrige** rimedia, invece, ad errori verificatisi nella stampa del provvedimento nella *Gazzetta Ufficiale*. I relativi comunicati sono pubblicati, ai sensi dell'art. 8 del decreto del Presidente della Repubblica 28 dicembre 1985, n. 1092, e degli articoli 14, e 18 del decreto del Presidente della Repubblica 14 marzo 1986, n. 217.

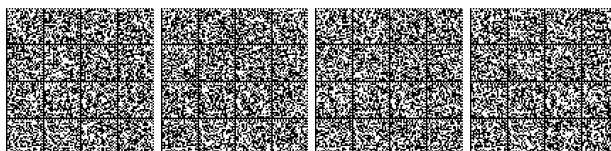
ERRATA-CORRIGE

Comunicato relativo alla determina 10 luglio 2013 dell'Agenzia del territorio, recante: «Accertamento periodo di mancato funzionamento del Servizio pubblicità immobiliare delle Circoscrizioni di Roma 1 e Roma 2 – Ufficio Provinciale di Roma – Territorio.». (Determina pubblicata nella *Gazzetta Ufficiale* – serie generale – n. 171 del 23 luglio 2013).

La determina citata in epigrafe, pubblicata nella sopra indicata *Gazzetta Ufficiale* è stata erroneamente inserita fra i provvedimenti emanati dall'Agenzia del territorio. Pertanto alla pagina II del Sommario, prima colonna e alla pag. 25, prima colonna, dove è scritto: *«Agenzia del territorio»*, leggasi: *«Agenzia delle entrate»*.

13A06450

MARCO MANCINETTI, *redattore* DELIA CHIARA, *vice redattore*

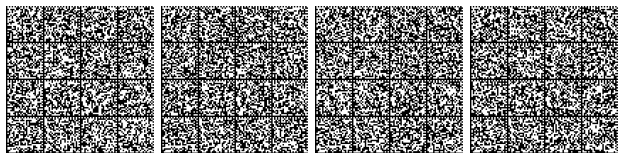
(WI-GU-2013-GU1-172) Roma, 2013 - Istituto Poligrafico e Zecca dello Stato S.p.A.

MODALITÀ PER LA VENDITA

La «Gazzetta Ufficiale» e tutte le altre pubblicazioni dell'Istituto sono in vendita al pubblico:

- **— presso l'Agenzia dell'Istituto Poligrafico e Zecca dello Stato S.p.A. in ROMA, piazza G. Verdi, 1 - 00198 Roma ☎ 06-85082147**
- **— presso le librerie concessionarie riportate nell'elenco consultabile sui siti www.ipzs.it e www.gazzettaufficiale.it.**

L'Istituto conserva per la vendita le Gazzette degli ultimi 4 anni fino ad esaurimento. Le richieste per corrispondenza potranno essere inviate a:

Istituto Poligrafico e Zecca dello Stato
Direzione Marketing e Vendite
Via Salaria, 1027
00138 Roma
fax: 06-8508-3466
e-mail: informazioni@gazzettaufficiale.it

avendo cura di specificare nell'ordine, oltre al fascicolo di GU richiesto, l'indirizzo di spedizione e di fatturazione (se diverso) ed indicando i dati fiscali (codice fiscale e partita IVA, se titolari) obbligatori secondo il DL 223/2007. L'importo della fornitura, maggiorato di un contributo per le spese di spedizione, sarà versato in contanti alla ricezione.

GAZZETTA UFFICIALE
DELLA REPUBBLICA ITALIANA

CANONI DI ABBONAMENTO (salvo conguaglio)
validi a partire dal 1° GENNAIO 2013

GAZZETTA UFFICIALE - PARTE I (legislativa)

		CANONE DI ABBONAMENTO	
Tipo A	Abbonamento ai fascicoli della serie generale, inclusi tutti i supplementi ordinari:		
	*(di cui spese di spedizione € 257,04)**	- annuale	€ **438,00**
	*(di cui spese di spedizione € 128,52)**	- semestrale	€ **239,00**
Tipo B	Abbonamento ai fascicoli della serie speciale destinata agli atti dei giudizi davanti alla Corte Costituzionale:		
	*(di cui spese di spedizione € 19,29)**	- annuale	€ **68,00**
	*(di cui spese di spedizione € 9,64)**	- semestrale	€ **43,00**
Tipo C	Abbonamento ai fascicoli della serie speciale destinata agli atti della UE:		
	*(di cui spese di spedizione € 41,27)**	- annuale	€ **168,00**
	*(di cui spese di spedizione € 20,63)**	- semestrale	€ **91,00**
Tipo D	Abbonamento ai fascicoli della serie destinata alle leggi e regolamenti regionali:		
	*(di cui spese di spedizione € 15,31)**	- annuale	€ **65,00**
	*(di cui spese di spedizione € 7,65)**	- semestrale	€ **40,00**
Tipo E	Abbonamento ai fascicoli della serie speciale destinata ai concorsi indetti dallo Stato e dalle altre pubbliche amministrazioni:		
	*(di cui spese di spedizione € 50,02)**	- annuale	€ **167,00**
	*(di cui spese di spedizione € 25,01)**	- semestrale	€ **90,00**
Tipo F	Abbonamento ai fascicoli della serie generale, inclusi tutti i supplementi ordinari, e dai fascicoli delle quattro serie speciali:		
	*(di cui spese di spedizione € 383,93)**	- annuale	€ **819,00**
	*(di cui spese di spedizione € 191,46)**	- semestrale	€ **431,00**

N.B.: L'abbonamento alla GURI tipo A ed F comprende gli indici mensili

CONTO RIASSUNTIVO DEL TESORO

Abbonamento annuo (incluse spese di spedizione) € **56,00**

PREZZI DI VENDITA A FASCICOLI
(Oltre le spese di spedizione)

Prezzi di vendita:		
	serie generale	€ 1,00
	serie speciali (escluso concorsi), ogni 16 pagine o frazione	€ 1,00
	fascicolo serie speciale, *concorsi*, prezzo unico	€ 1,50
	supplementi (ordinari e straordinari), ogni 16 pagine o frazione	€ 1,00
	fascicolo Conto Riassuntivo del Tesoro, prezzo unico	€ 6,00

I.V.A. 4% a carico dell'Editore

PARTE I - 5ª SERIE SPECIALE - CONTRATTI PUBBLICI

*(di cui spese di spedizione € 128,06)**	- annuale	€ **300,00**
*(di cui spese di spedizione € 73,81)**	- semestrale	€ **165,00**

GAZZETTA UFFICIALE - PARTE II

*(di cui spese di spedizione € 39,73)**	- annuale	€ **86,00**
*(di cui spese di spedizione € 20,77)**	- semestrale	€ **55,00**

Prezzo di vendita di un fascicolo, ogni 16 pagine o frazione (oltre le spese di spedizione) € 1,00 (€ 0,83+ IVA)

Sulle pubblicazioni della 5° Serie Speciale e della Parte II viene imposta I.V.A. al 21%.

RACCOLTA UFFICIALE DEGLI ATTI NORMATIVI

Abbonamento annuo		€ **190,00**
Abbonamento annuo per regioni, province e comuni - SCONTO 5%		€ **180,50**
Volume separato (oltre le spese di spedizione)	€ 18,00	

I.V.A. 4% a carico dell'Editore

Per l'estero i prezzi di vendita (in abbonamento ed a fascicoli separati) anche per le annate arretrate, compresi i fascicoli dei supplementi ordinari e straordinari, devono intendersi raddoppiati. Per il territorio nazionale i prezzi di vendita dei fascicoli separati, compresi i supplementi ordinari e straordinari, relativi anche ad anni precedenti, devono intendersi raddoppiati. Per intere annate è raddoppiato il prezzo dell'abbonamento in corso. Le spese di spedizione relative alle richieste di invio per corrispondenza di singoli fascicoli, vengono stabilite, di volta in volta, in base alle copie richieste. Eventuali fascicoli non recapitati potrannno essere forniti gratuitamente entro 60 giorni dalla data di pubblicazione del fascicolo. Oltre tale periodo questi potranno essere forniti soltanto a pagamento.

N.B. - La spedizione dei fascicoli inizierà entro 15 giorni dall'attivazione da parte dell'Ufficio Abbonamenti Gazzetta Ufficiale.

RESTANO CONFERMATI GLI SCONTI COMMERCIALI APPLICATI AI SOLI COSTI DI ABBONAMENTO

* tariffe postali di cui alla Legge 27 febbraio 2004, n. 46 (G.U. n. 48/2004) per soggetti iscritti al R.O.C.